COMTREND CORPORATION

CT-5624

4-Port ADSL2+ Router

User Manual

Version A1.2, June 9, 2008

261085-005

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix C

Copyright

NOTE:	This document is subject to change without notice.

Table of Contents

Chapter 1 Introduction

The CT-5624 series ADSL2+ compact and high performance Ethernet router provides four 10/100 Ethernet Interfaces, and one ADSL line interface to access the Internet, incorporating LAN or Video on Demand over one ordinary telephone line, at speeds of up to 24 Mbps. It also has full routing capabilities to segment/route IP protocol and supports advanced security functions.

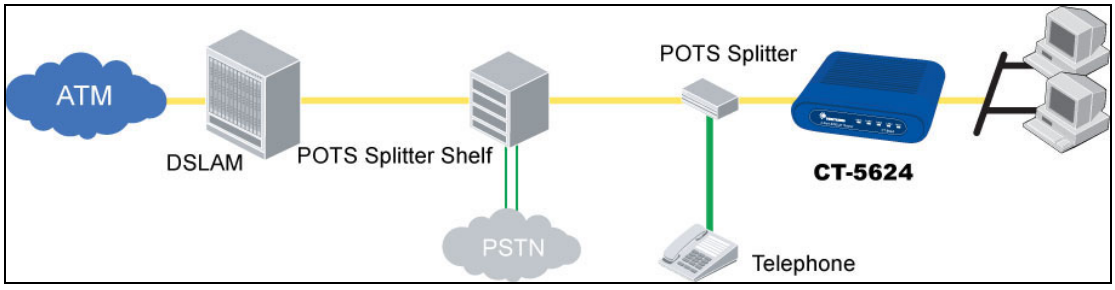
The CT-5624 is for ADSL over POTS (i.e. Annex A). The CT-5624 series can operate in router or bridge mode. In addition, the CT-5624 series protects all of your networked computers with advanced security technologies, such as virtual private networks (VPNs) with PPTP passthrough, L2TP passthrough, IPSec passthrough, and firewall.

FEATURES

- IP address filtering
- Dynamic IP assignment
- IGMP Proxy
- DNS Proxy
- Per-VC packet level QoS
- Embedded SNMP agent
- Remote configuration and upgrade
- FTP/TFTP server
- Static route/RIP v1/v2
- NAT/PAT
- DHCP Server/Client
- Auto PVC configuration
- Up to 8 VCs
- Web-based management
- Configuration backup and restore

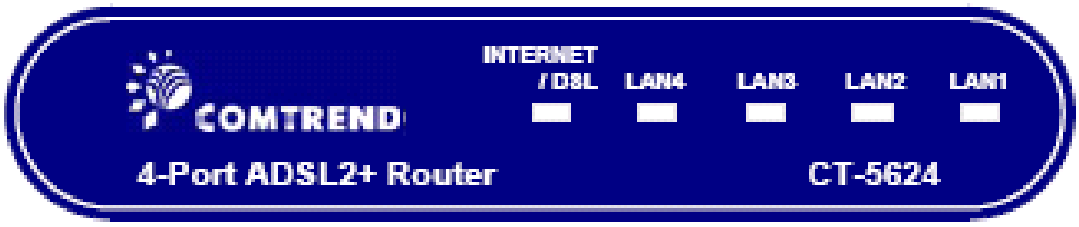
APPLICATION

The following diagram depicts the application of the CT-5624.



Chapter 2 Installation

Front Panel

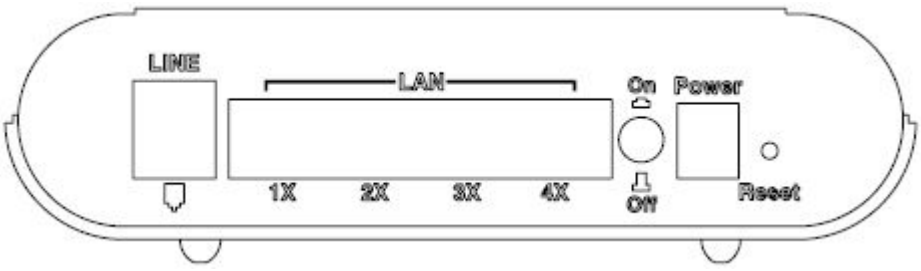


The front panel contains lights called LEDs that indicate the status of the unit.

Front Panel LEDs	
INTERNET/DSL	Red: No ADSL link
	Orange on: The ADSL connection is established and the device had attempted to obtain an IP address but failed (reason: no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
	Red/Orange interlacing: the DSL is training.
	Green on: The ADSL connection is established and Internet is established.
	Off: Modem power off
LAN 1x-4X (Green)	On: The Ethernet connection is established. Off: The Ethernet connection is not established. Blink: Data transmitting or receiving.

Rear Panel

The rear panel contains the ports for the unit's data and power connections.



Label	Function
LINE	RJ-11 connector: Connects the device to a telephone jack using the supplied cable
LAN 1-4	RJ-45 connector: Connects the device to your PC LAN port, or to the uplink port on your LAN hub. Use the Ethernet cable provided.
Power	Connects to the power adapter.

Chapter 3 Connecting the Hardware

You connect the device to the phone jack, the power outlet, and your computer or network.

Step 1. Connect the ADSL cable and optional telephone.
Connect one end of the provided phone cable to the port labeled ADSL on the rear panel of the device. Connect the other end to your wall phone jack. You can attach a telephone line to the device. This is helpful when the ADSL line uses the only convenient wall phone jack. If desired, connect the telephone cable to the port labeled PHONE.

NOTE:	Although you use the same type of cable, The ADSL/PHONE ports are not interchangeable. Do not route the ADSL connection through the PHONE port.

Step 2. Connect the Ethernet cable.
If you are connecting a LAN to the 4-port ADSL/Ethernet router, attach one end of a provided Ethernet cable to a regular hub port and the other to the Ethernet port on the router.

Step 3. Attach the power connector.
Connect the AC power adapter to the PWR connector on the back of the device and plug in the adapter to a wall outlet or power strip.

Step 4. Turn on the Router and power up your systems.
Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 5. Configure the Router with the Web User Interface (WUI).
Chapters 5 through 9 show how to configure the CT-5624 to meet your needs.

Step 6. Save the configurations and Reboot.
To make the settings you configured on the router take effect.

Chapter 4 Login via the Web Browser

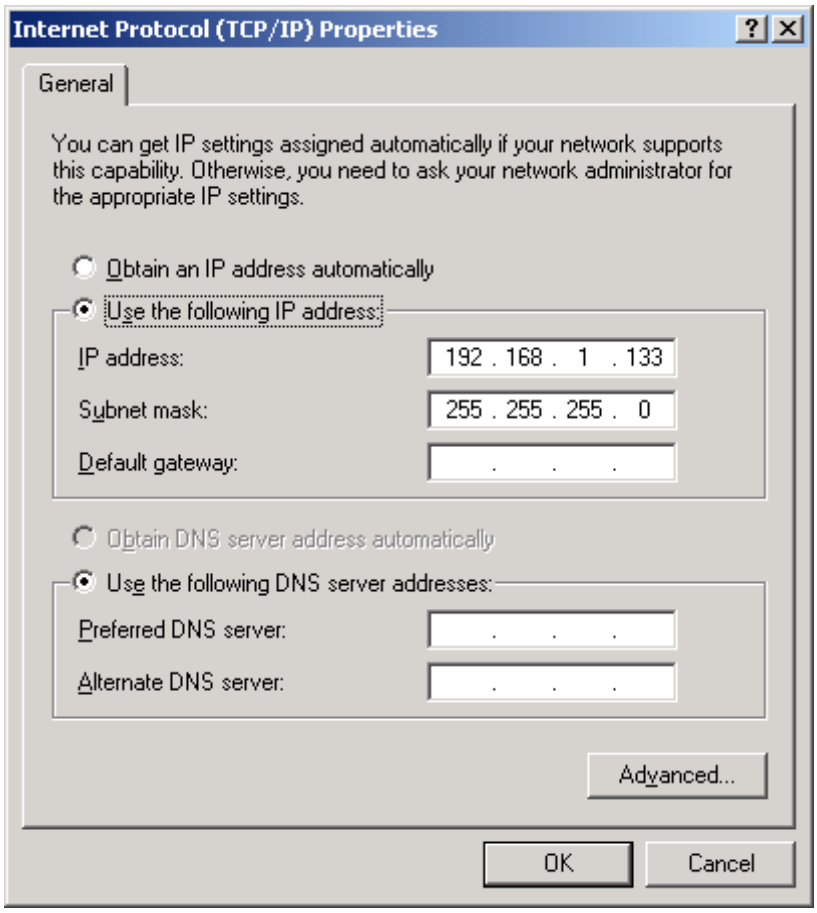
This section describes how to manage the router via a Web browser via the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. The Web page is best viewed with Microsoft Internet Explorer 5.0 and later.

4.1 IP Configuration

The default IP address of the CT-5624 (LAN port) is 192.168.1.1. To configure the CT-5624 for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

STEP 1: Right click on the Local Area Connection under the Network and Dial-Up connection window and select Properties.

STEP 2: Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24.



STEP 3: Click **OK** to submit the settings.

STEP 4: Start your Internet browser with the default IP address 192.168.1.1.

4.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-5624. To log on to the system from the Web browser, follow the steps below:

STEP 1: Start your Internet browser. Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.1, type **http://192.168.1.1**

STEP 2: You will be prompted to enter your user name and password. Type **root** in the user name and **12345** in the password field, and click **OK**. These values can be changed later in the Web User Interface by selecting the **Management** link.

STEP 3: After successfully logging in, you will reach the Quick Setup menu.

4.3 Default Settings

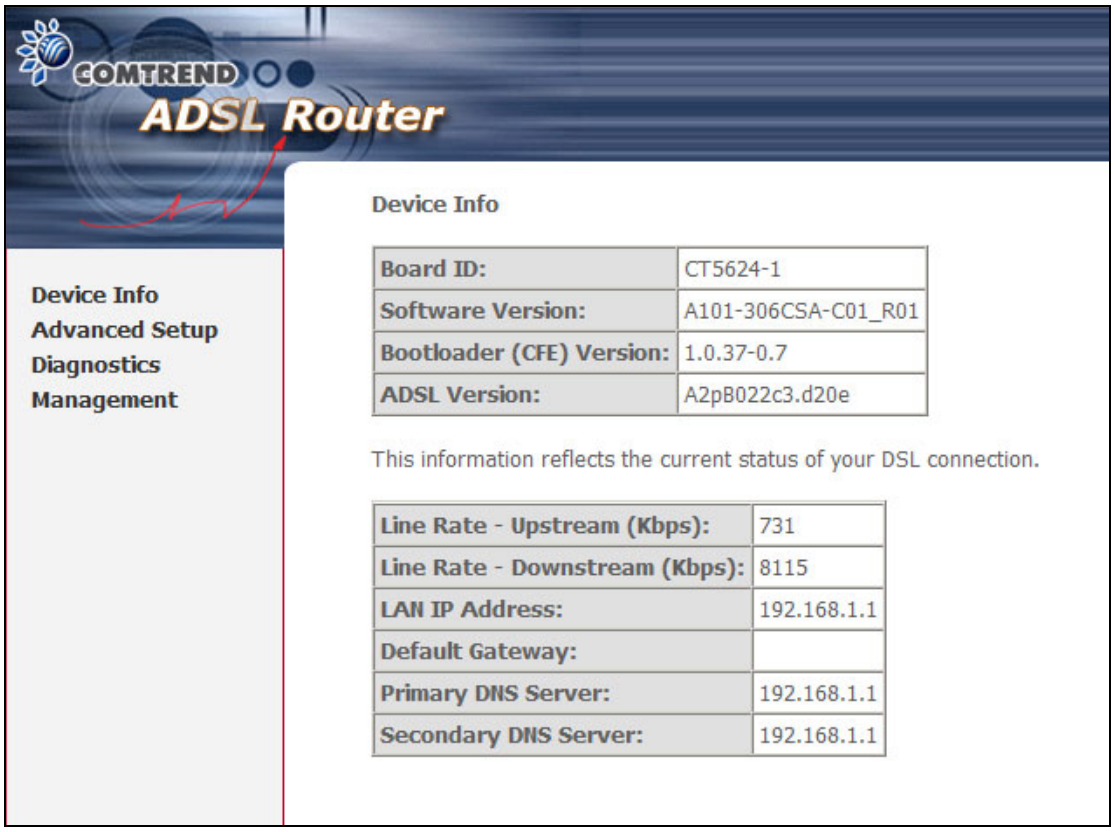
The following default settings are present when setting up the router for the first time. The PC running the browser can be attached to the Ethernet.

- One PPPoE PVC (VPI=8, VCI=35)
- NAT Enabled and Firewall Disabled
- DHCP server on LAN interface: Enabled
- WAN IP address: None
- LAN port IP address: 192.168.1.1
- Local administrator account name: root
- Local administrator account password: 12345
- Remote WAN access: Enabled
- Remote WAN access account name: root
- Remote WAN access account password: 12345

Technical Note:
During power on initialization, the router initializes all configuration attributes to default values. It will then read the configuration profile from the Permanent Storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in Permanent Storage can be created via the Web User Interface (WUI), the console, telnet client or other management tools. The factory default configuration can be restored either by pushing the reset button for more than five seconds, or by clicking the Restore Default Configuration option in the Restore Settings screen.

Chapter 5 Device Information

The Summary screen appears as shown below.



NOTE: The selections available on the main menu are based upon the configured connections and the active user account.

5.1 WAN

This screen displays the configured PVC(s) and their status.

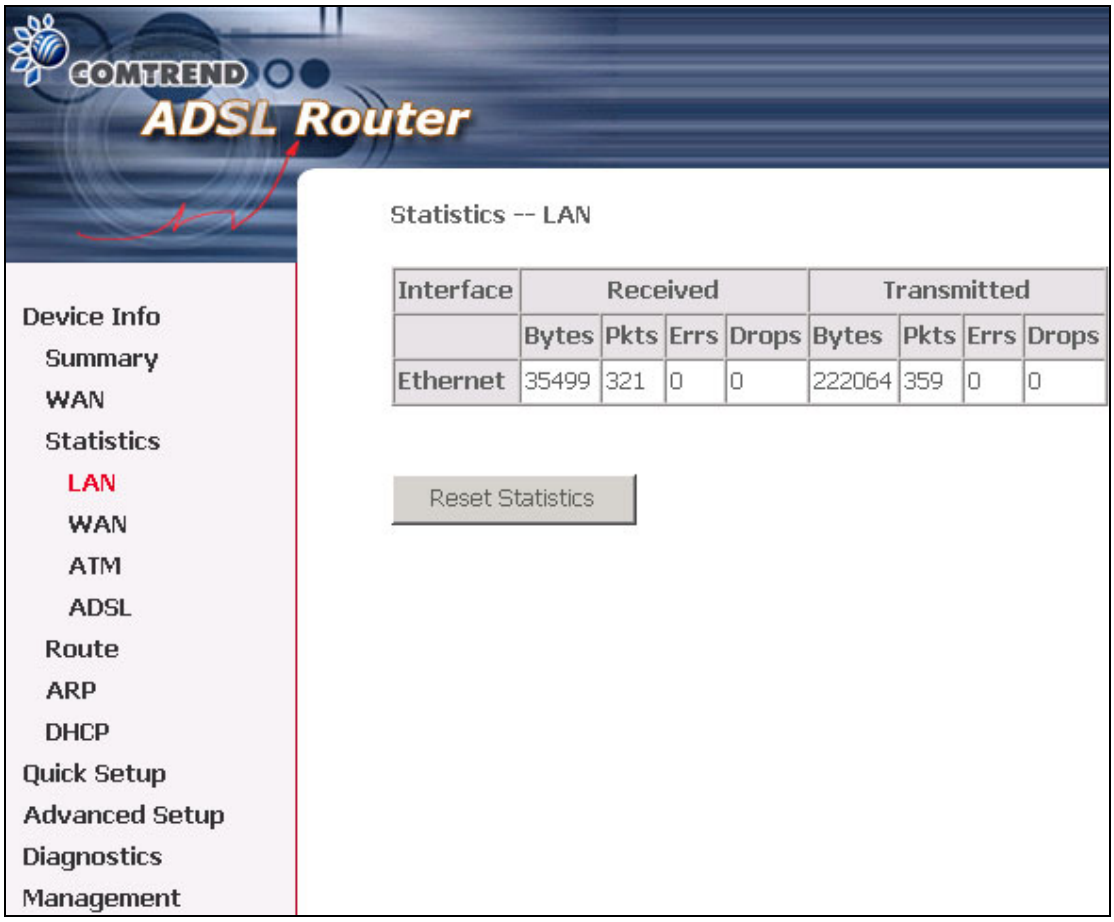
VPI/VCI	Shows the values of the ATM VPI/VCI
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the state of the IGMP function
NAT	Shows if NAT is Enabled or Disabled
FIREWALL	Shows if Firewall is Enabled or Disabled
QoS	Shows if QoS (quality of service) is Enabled or Disabled
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

5.2 Statistics

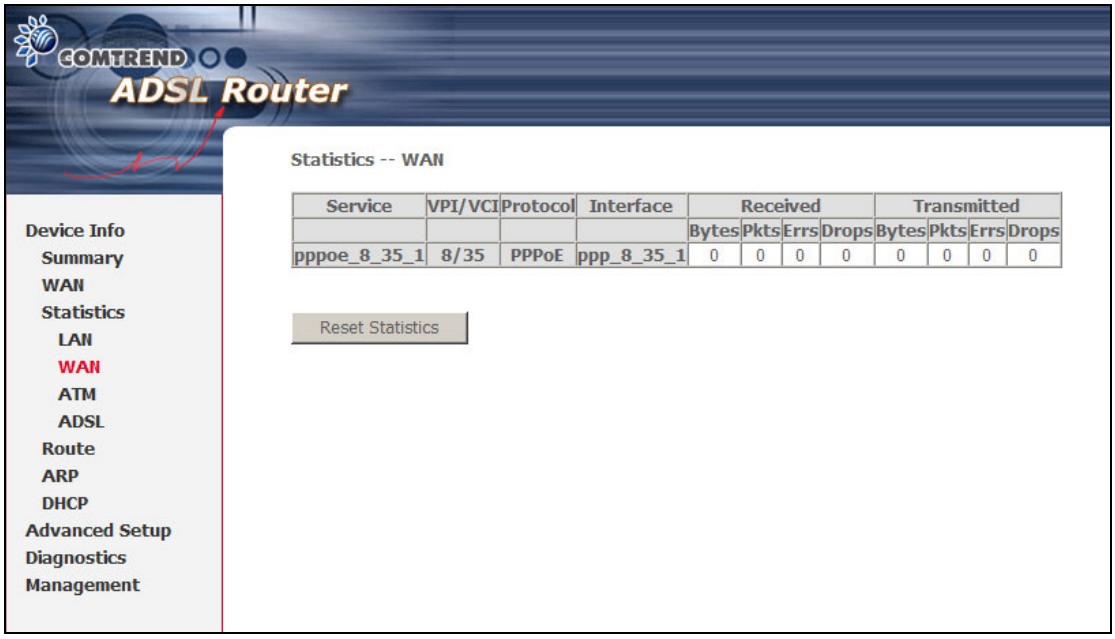
Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM and ADSL. All statistics screens are updated every 15 seconds.

5.2.1 LAN Statistics

The Network Statistics screen shows interface statistics for the Ethernet interface. (The Network Statistics screen shows interface statistics for LAN of Ethernet interface. Here provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



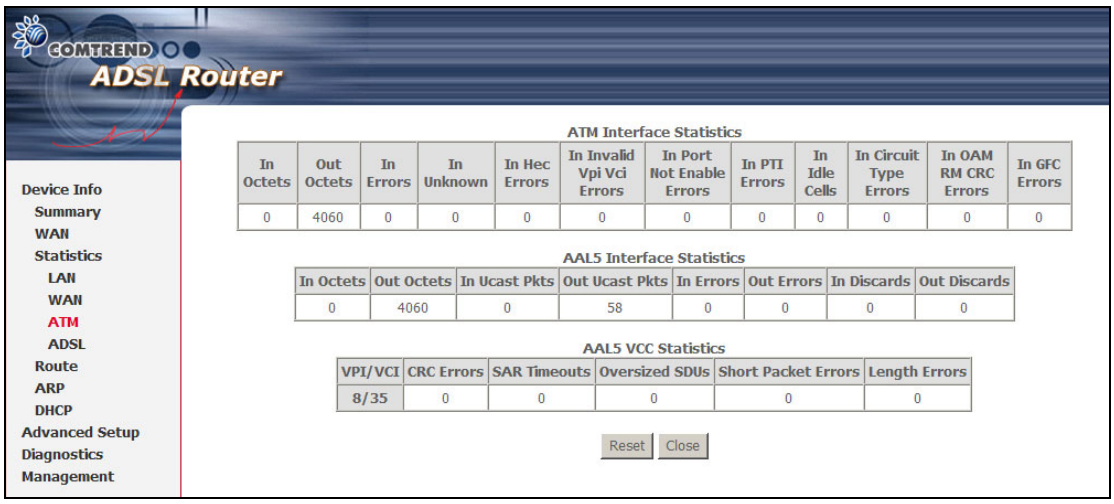
5.2.2 WAN Statistics



Service		Shows the service type
VPI/VCI		Shows the values of the ATM VPI/VCI
Protocol		Shows the connection type, such as PPPoE, PPPoA, etc.
Interface		Shows connection interfaces
Received/Transmitted	- Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in Byte Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) packets with errors Rx/TX (receive/transmit) dropped packets

5.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enabled Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In Oam RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

ATM AAL5 Layer Statistics over ADSL interface

Field	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucst Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmissions
In Errors	Number of received AAL5/AAL0 CPCS PDUs received that contain an error. The types of errors counted include CRC-32 errors.

Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

ATM AAL5 LAYER STATISTICS FOR EACH VCC OVER ADSL INTERFACE

Field	**Descriptions**
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

5.2.4 ADSL Statistics

The following figure shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button refreshes the ADSL statistics.

Statistics -- ADSL

Mode:		ADSL2+
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	6.1	6.0
Attenuation (dB):	3.5	1.6
Output Power (dBm):	12.4	17.8
Attainable Rate (Kbps):	20716	1
Rate (Kbps):	20340	1183
MSGc (number of bytes in overhead channel message):	74	11
B (number of bytes in Mux Data Frame):	254	36
M (number of Mux Data Frames in FEC Data Frame):	1	1
T (Mux Data Frames over sync bytes):	2	4
R (number of check bytes in FEC Data Frame):	0	0
S (ratio of FEC over PMD Data Frame length):	0.4004	0.9933
L (number of bits in PMD Data Frame):	5095	298
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	9581	9565
Super Frame Errors:	1	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	1	0
OCD Errors:	1	0
LCD Errors:	0	0
Total Cells:	7358009	0
Data Cells:	218	0
Bit Errors:	0	0
Total ES:	1	0
Total SES:	0	0
Total UAS:	16	0

ADSL BER Test Reset Statistics

Field	Description
Mode	T1.413, G.lite, G.DMT, ADSL2/2+ or Re-ADSL
Type	Channel type Interleave or Fast
Line Coding	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2, Annex L and Annex M
Status	Lists the status of the DSL link
Link Power State	Link output power state.

SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

In G.DMT mode, the following section is inserted.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

In ADSL2+ mode, the following section is inserted.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

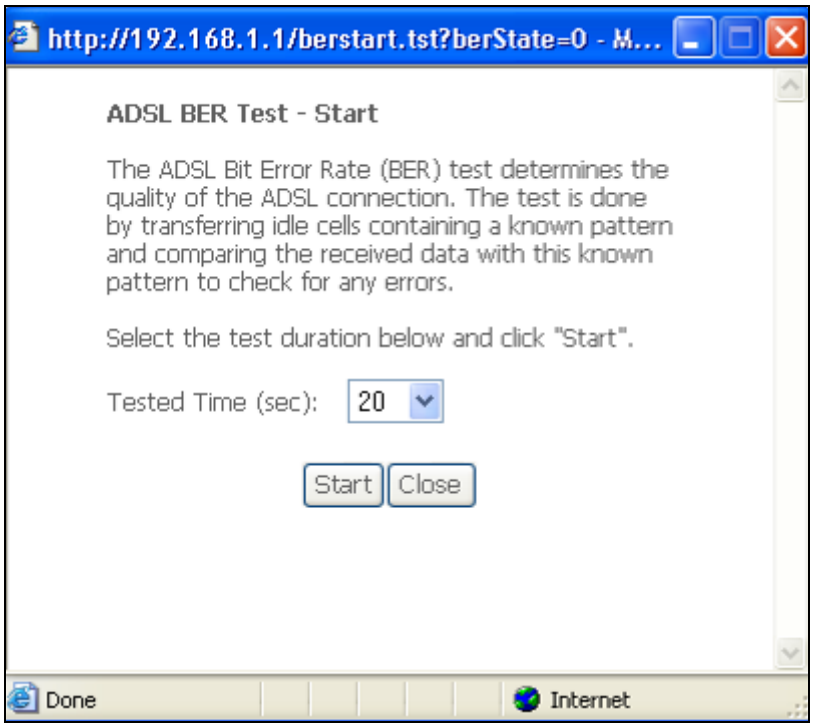
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle and data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

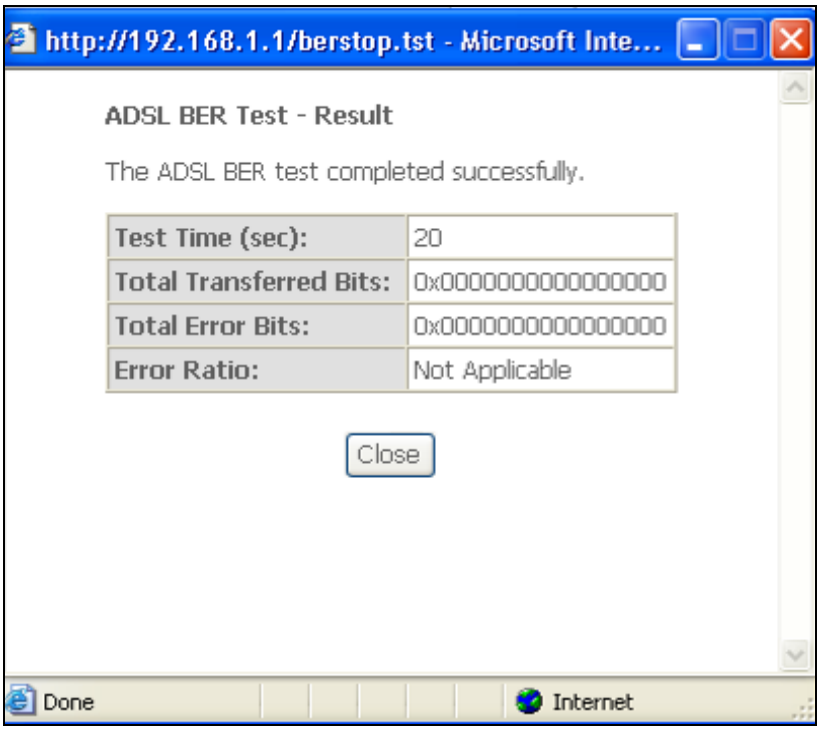
In ADSL2+ mode, the following section is inserted.

Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

Within the ADSL Statistics window, a Bit Error Rate (BER) test can be started using the **ADSL BER Test** button. A small window will open when the button is pressed; it will appear as shown below. Click **Start** to start the test or **Close**.

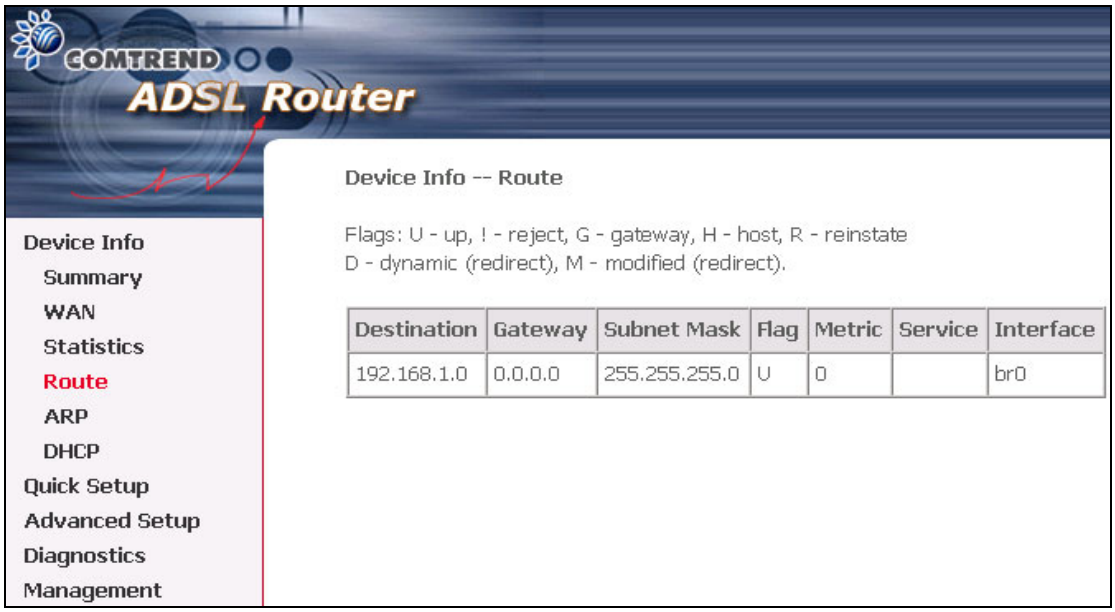


If the test is successful, the pop-up window will display as follows.



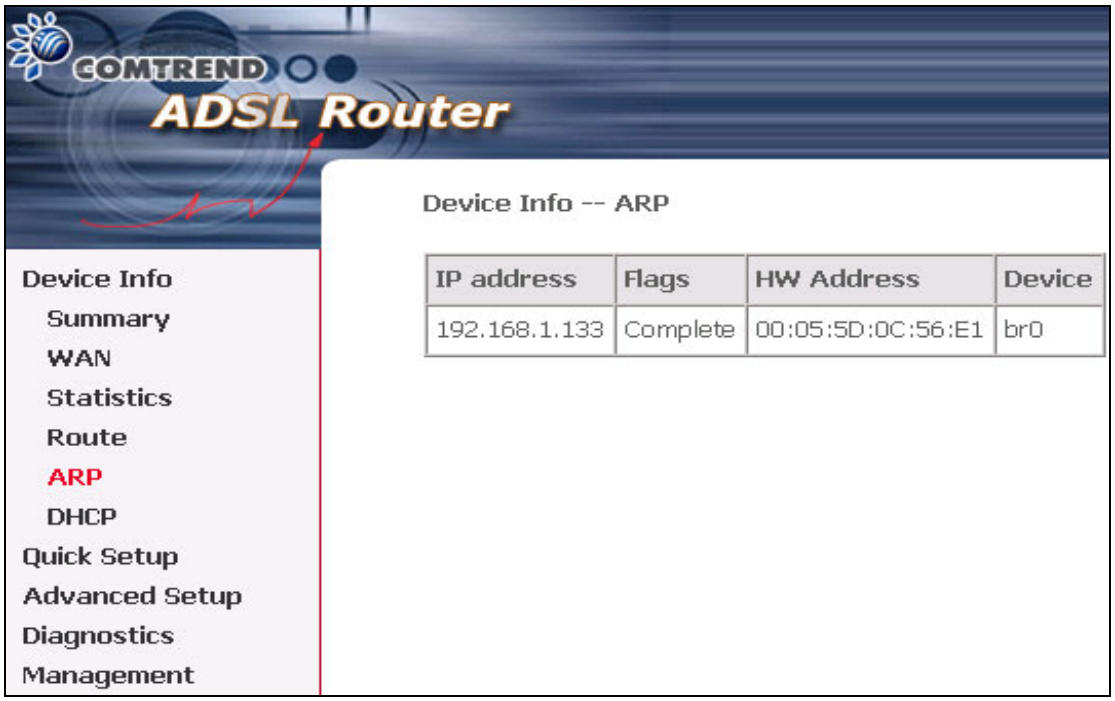
5.3 Route

Choose **Route** to display the routes that the route information has learned.



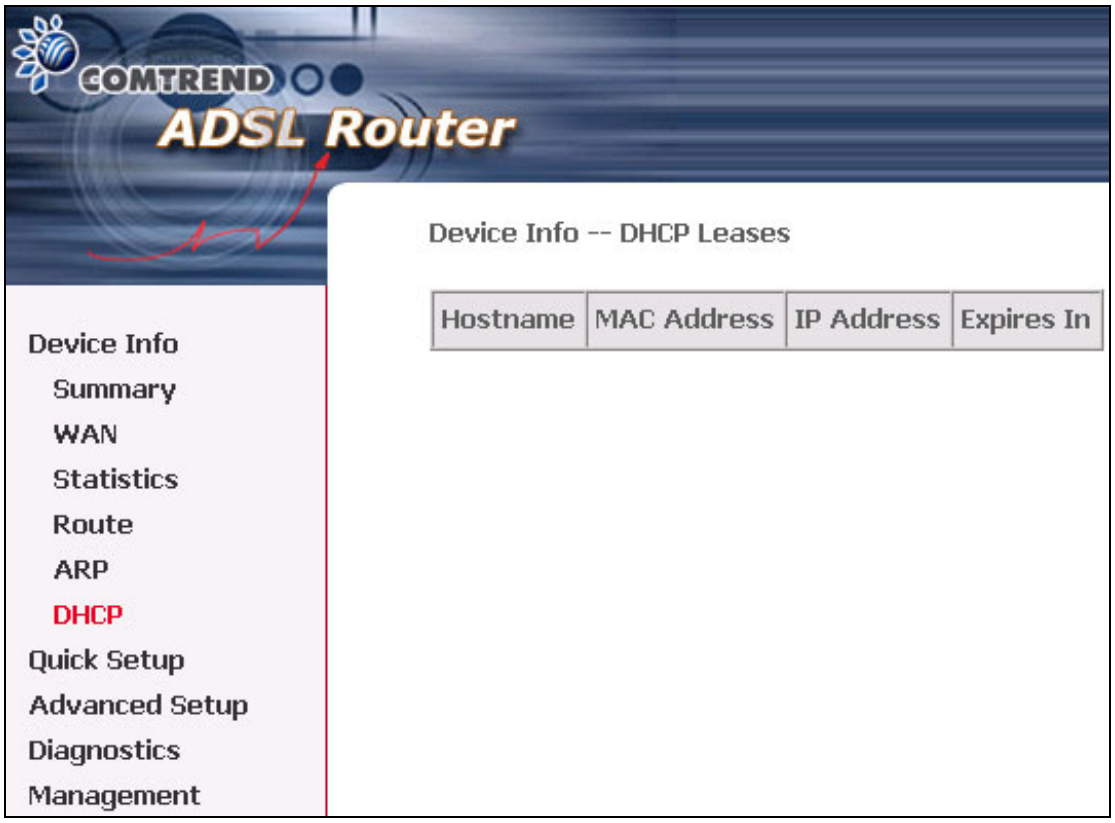
5.4 ARP

Click **ARP** to display the ARP information.



5.5 DHCP

Click **DHCP** to display the DHCP information.



Chapter 6 Quick Setup

The Quick Setup allows the user to configure the ADSL router for DSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

The CT-5624 ADSL router supports the following five network operating modes over an ATM PVC WAN interface.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-5624 is to run the PPPoE client. The CT-5624 can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge In PPPoE mode, CT-5624 also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client fro non-PPPoE LAN devices. NAT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network-operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

Note: Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

6.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

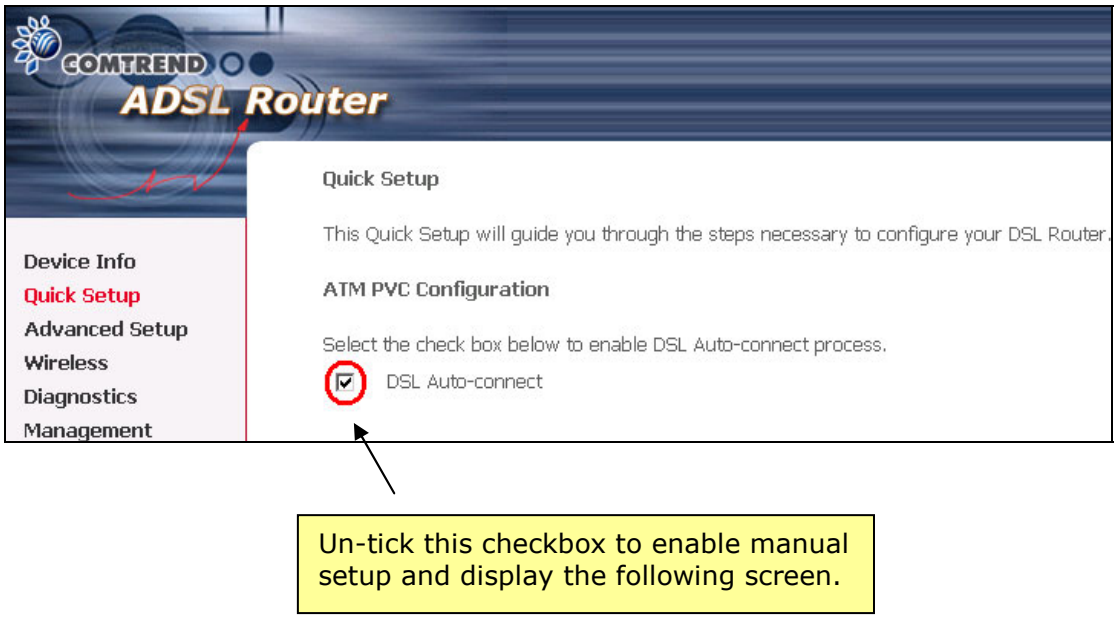
1. Select **Quick Setup** to display the DSL Quick Setup screen.

2. Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.

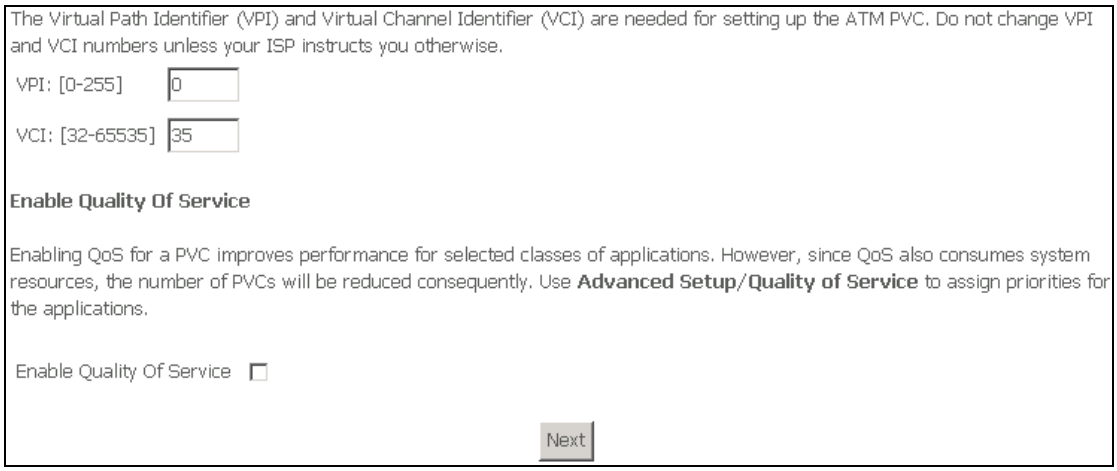
3. After the settings are complete, you can use the ADSL service.

6.2 Manual Quick Setup

STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.



Un-tick this checkbox to enable manual setup and display the following screen.

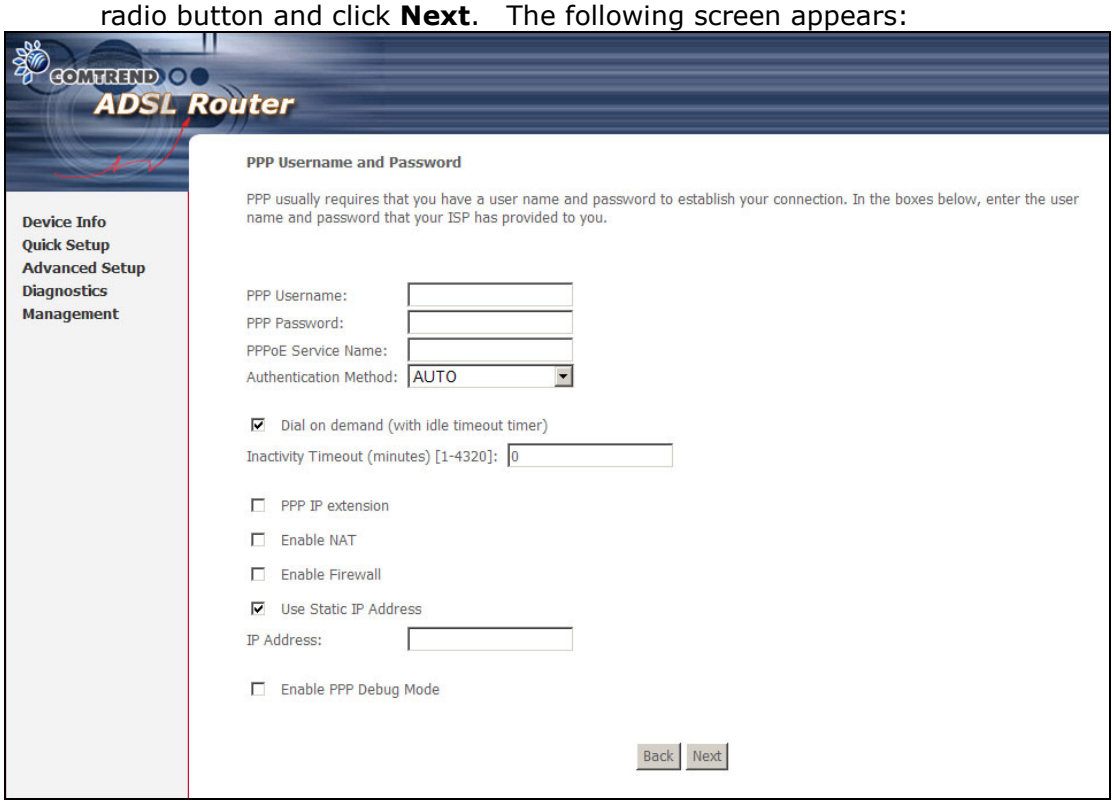


STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Select Enable Quality Of Service if required. Enabling IP QoS for a PVC improves performance for selected classes of applications. However, since IP QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications. Click **Next**.

STEP 3: Choosing different connection types pops up different settings requests. Enter appropriate settings that are requested by your service provider. The following descriptions state each connection type setup separately. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click **Next** to go to the next step.

6.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

1. Select the **PPP over ATM (PPPoA)** or **PPP over Ethernet (PPPoE)** radio button and click **Next**. The following screen appears:



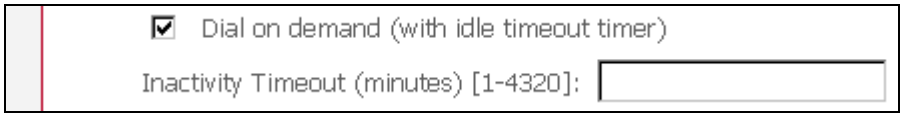
PPP Username/PPP Password
Give "PPP Username", "PPP Password" and "PPPoE Service Name", then select the "Authentication Method" (AUTO/PAP/CHAP/MSCHAP). Please contact your ISP for the information. The WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

PPPoE service name
For PPPoE service, PADI requests contain a service name-tag. Some PPPoE servers (or BRAS) of ISP check this service name-tag for connection.

Encapsulation Mode
Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

Disconnect if no activity
The CT-5624 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.



PPP IP Extension
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.
The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL router has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Firewall checkbox: If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Use Static IP Address
Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address.

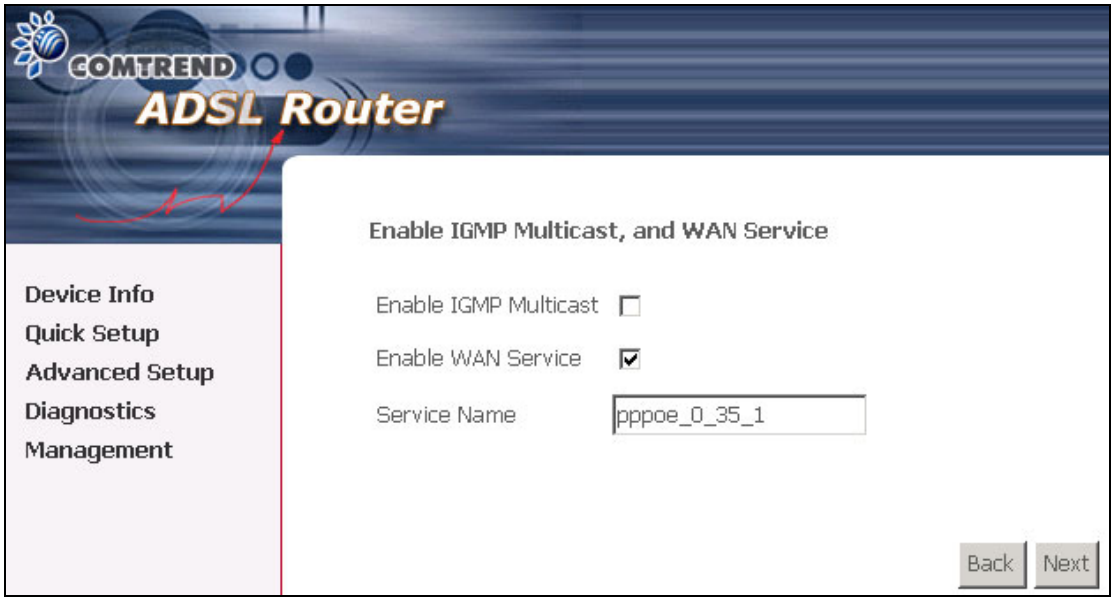
Enable PPP Debug Mode
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

2. Click **Next** to display the screen on the following page.

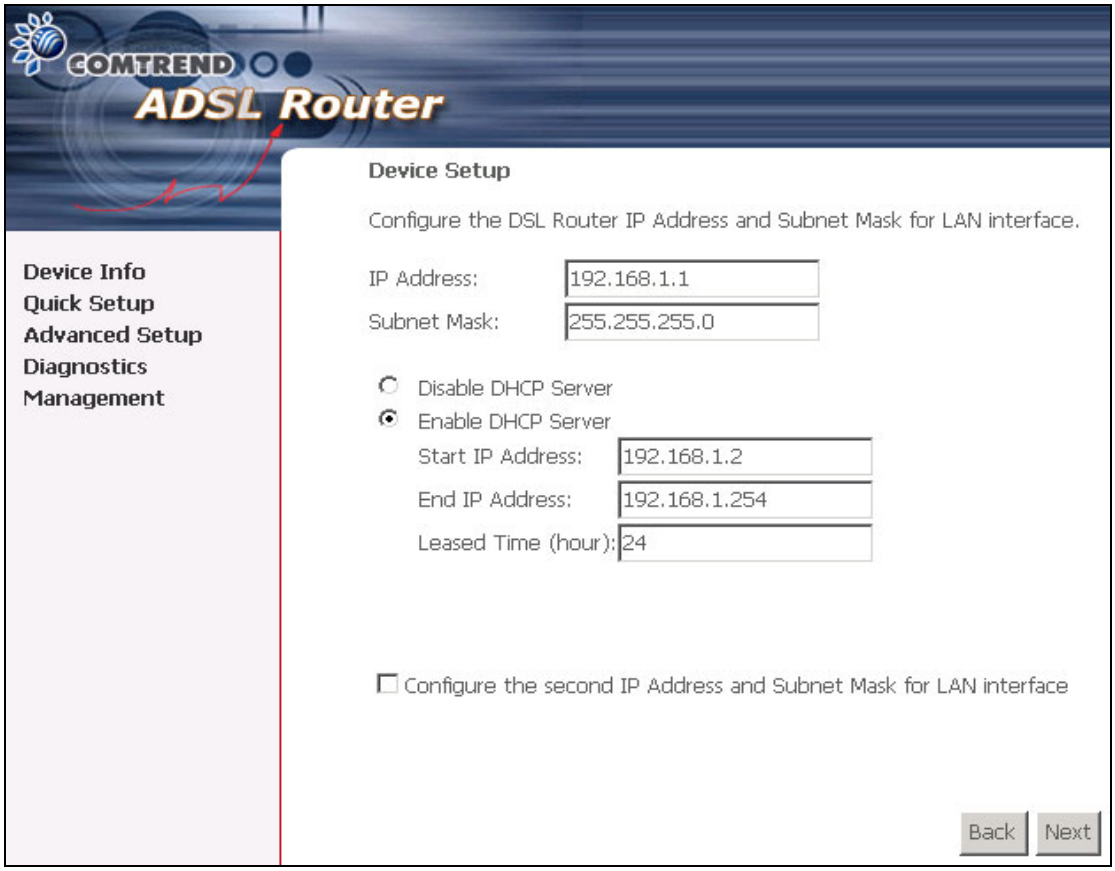
Enable IGMP Multicast checkbox: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service checkbox: Tick this item to enable the ATM service. Untick it to stop the ATM service.

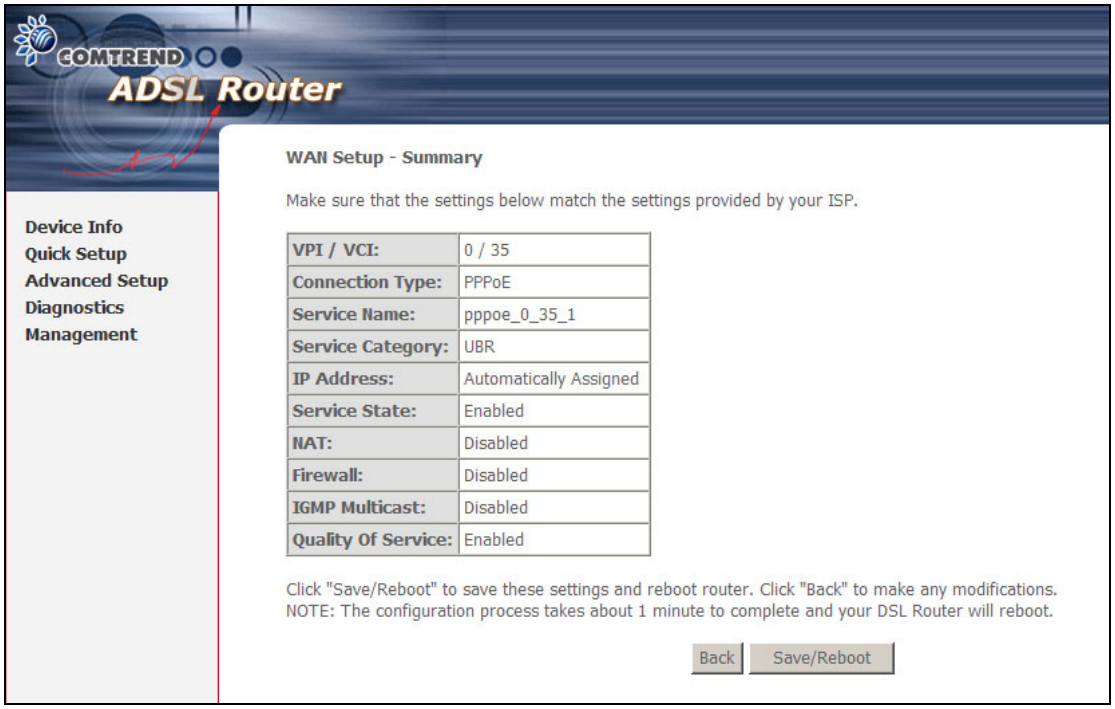
Service Name: This is user-defined.



3. After entering your settings, select **Next**. The following screen appears. This page allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this ADSL router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP leased time.



4. Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

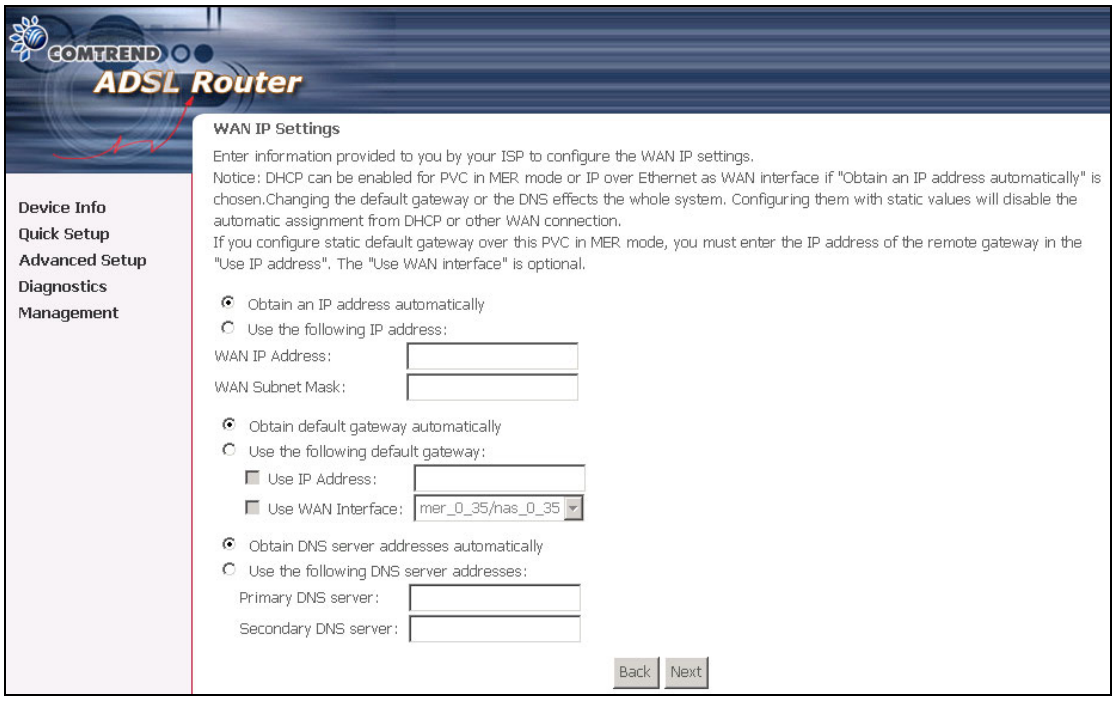


5. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5624 is ready for operation and the LEDs display as described in the LED description tables.

6.2.2 MAC Encapsulation Routing (MER)

To configure MER, do the following.

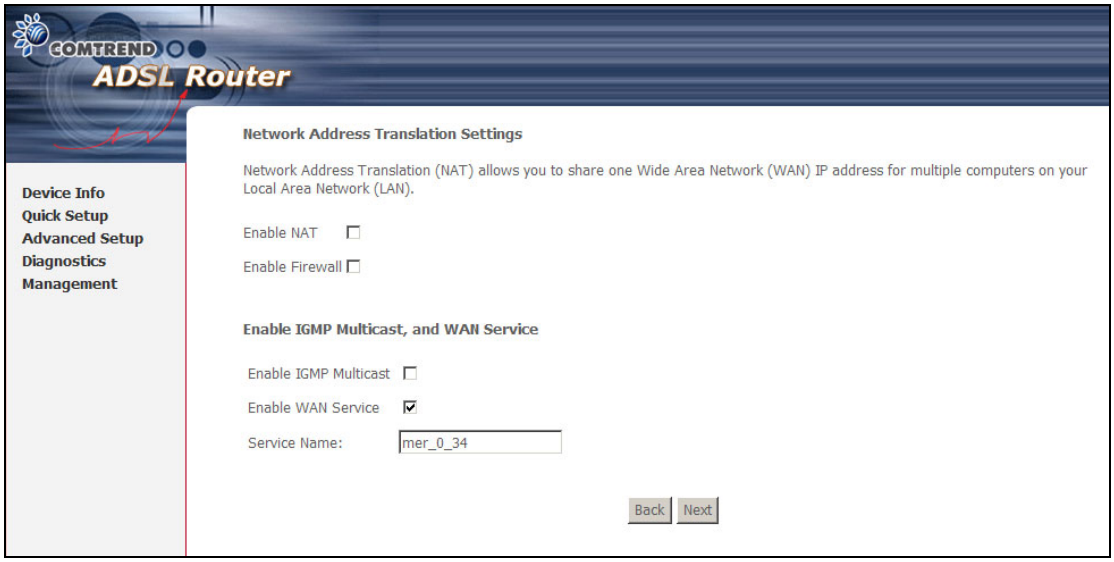
1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index provided by the ISP and click **Next.**
3. Select the MAC Encapsulation Routing (MER) radio button, and click **Next**. The following screen appears.



Enter information provided to you by your ISP to configure the WAN IP settings.

NOTE:	DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. For static default gateway you must enter the IP address in the "Use IP address" field. The "Use WAN interface" field is optional. The ISP should provide this information to you.

4. Click **Next** to display the following screen.



Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

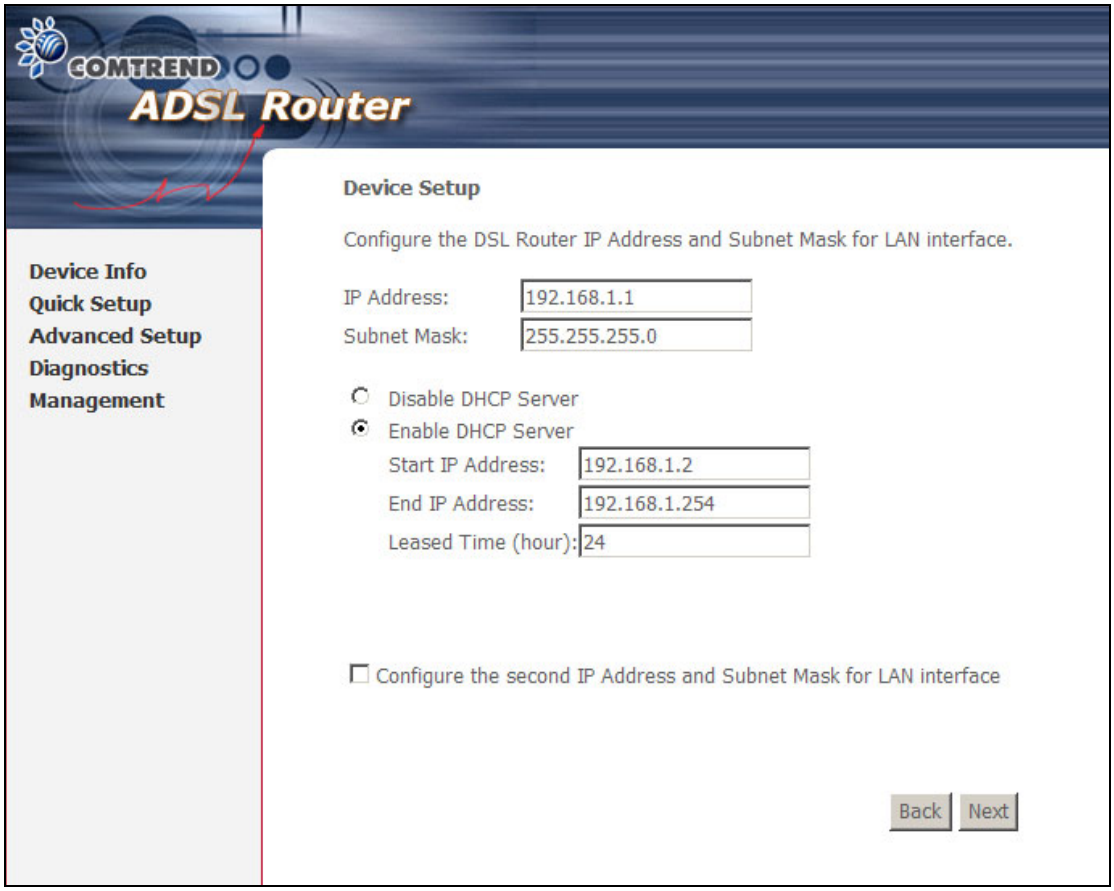
Enable Firewall checkbox: If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

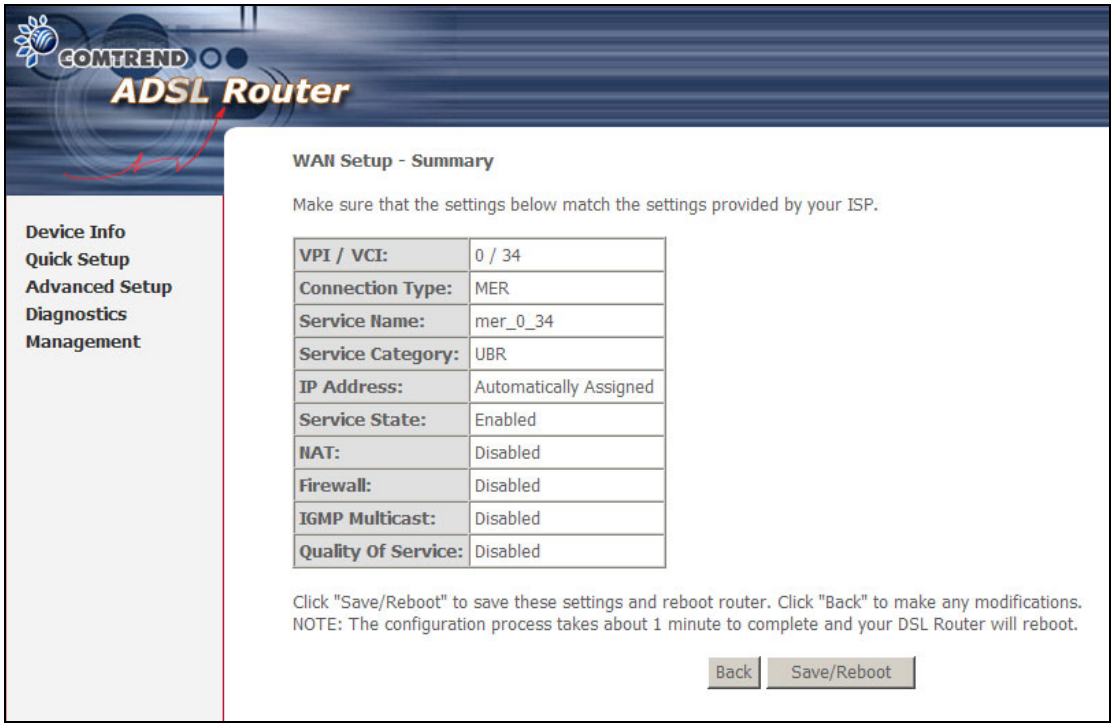
Service Name: This is User-defined.

5. Upon completion, click **Next**. The following screen appears.



The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server** and enter the Start and End IP address and the DHCP Leased Time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

6. After entering your settings, select **Next** to display the following screen. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

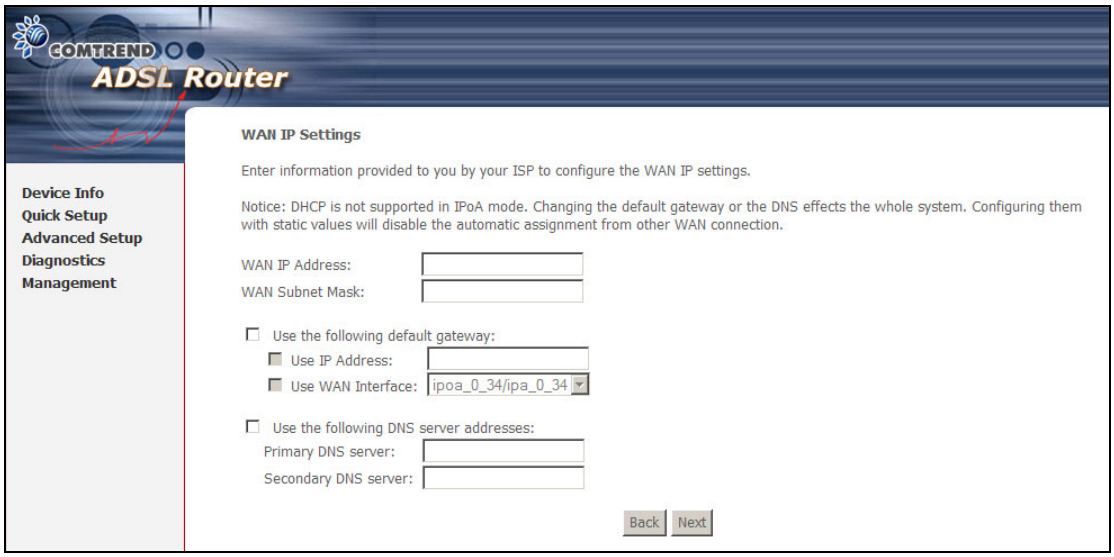


7. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5624 is ready for operation and the LEDs display as described in the LED description tables.

6.2.3 IP Over ATM

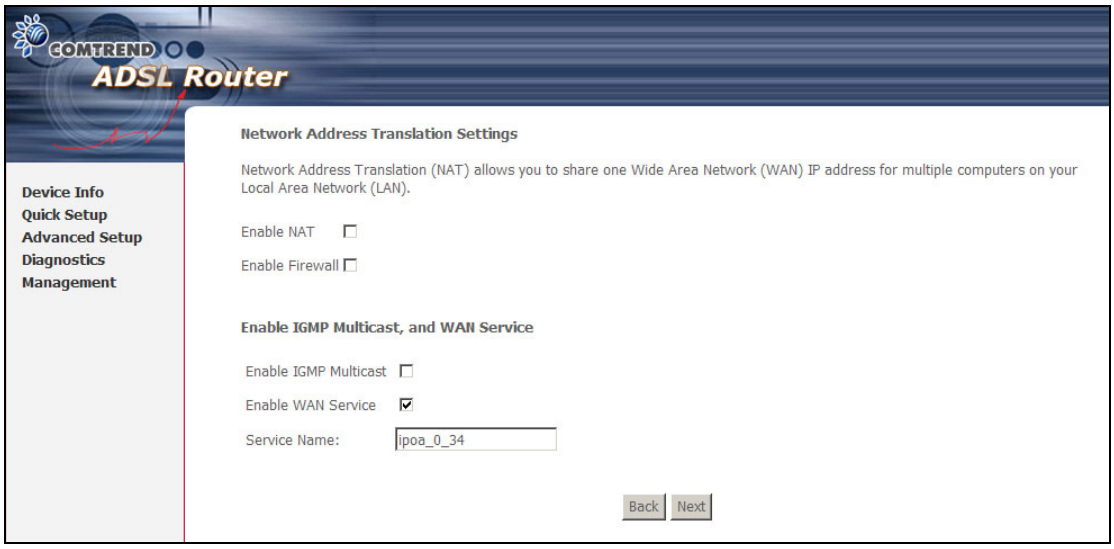
To configure IP Over ATM,

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type the VPI and VCI values provided by the ISP and click **Next**.
4. Select the IP over ATM (IPoA) radio button and click **Next**. The following screen appears.



NOTE:	DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup, and the DNS server addresses provided by the ISP.

5. Click **Next**. The following screen appears.



Enable NAT checkbox
If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side (i.e the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

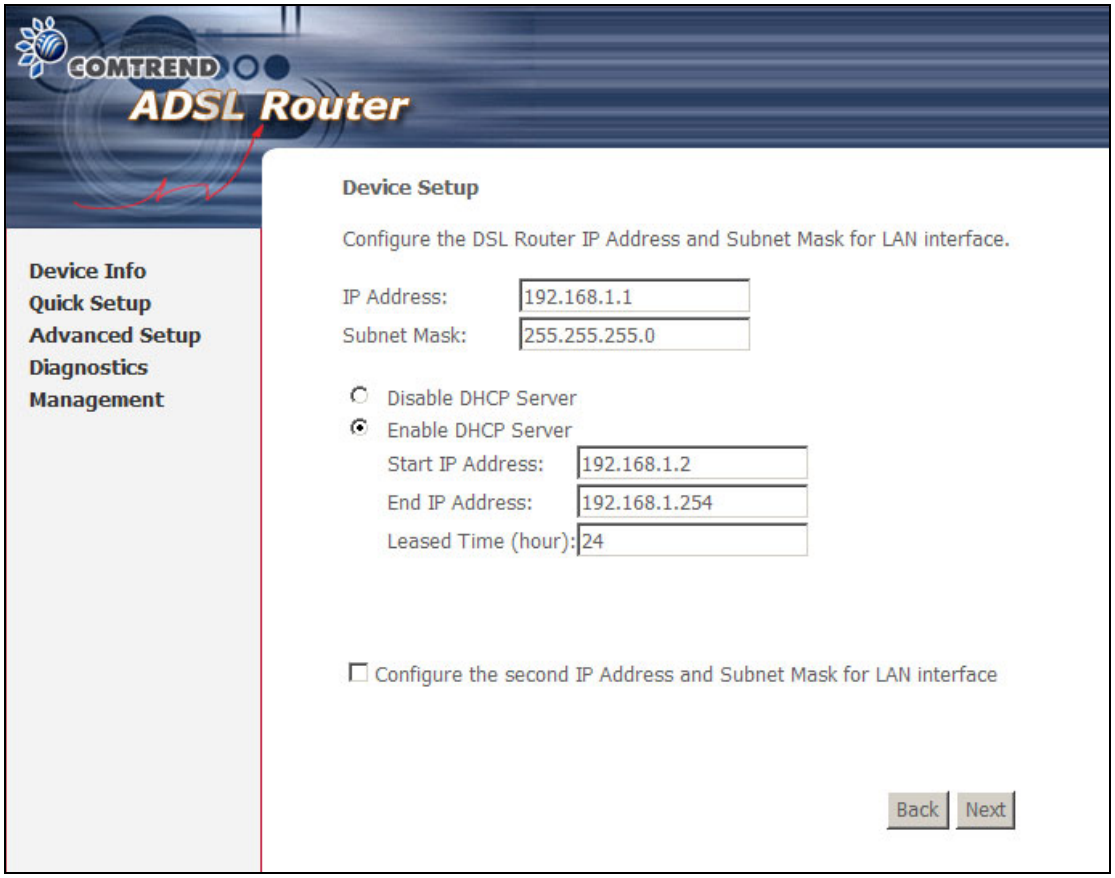
Enable Firewall checkbox
If the firewall checkbox is selected, the Security submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Security submenu will not be displayed on the left main panel.

Enable IGMP Multicast: Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable the WAN service. If this item is not selected, you will not be able to use the WAN service.

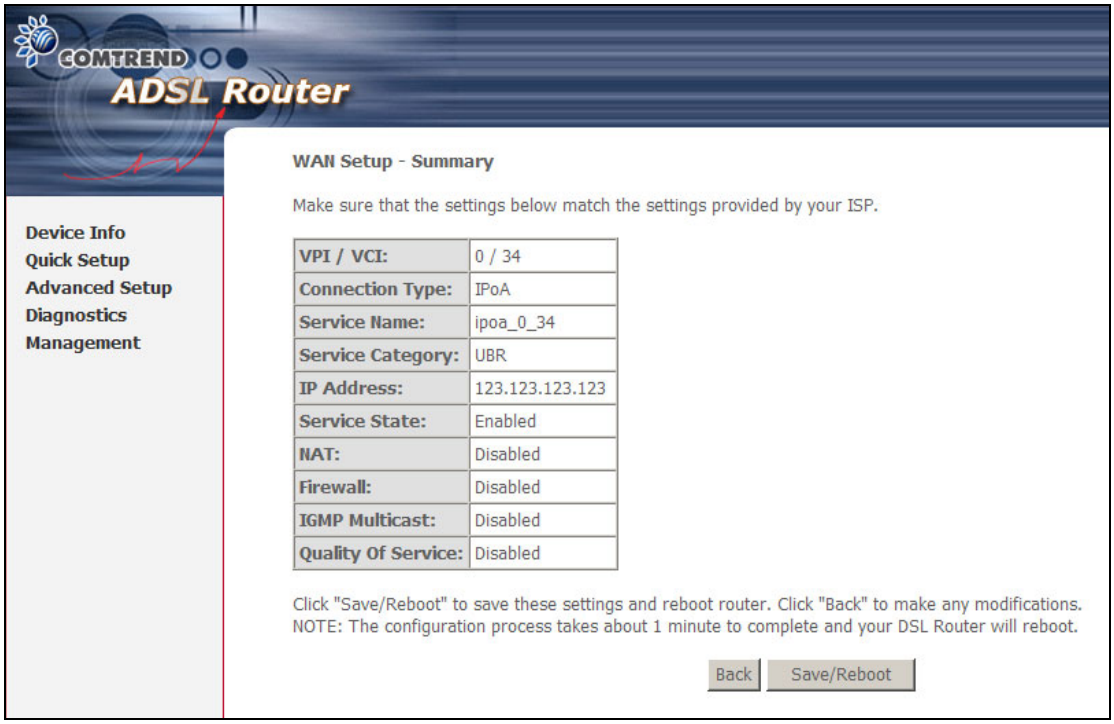
Service Name: This is User-defined.

6. Click **Next** to display the following screen. The Device Setup page allows the user to configure the LAN interface IP address and DHCP server if the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.



The user must configure the IP Address and the Subnet Mask. To use the DHCP service on the LAN, select the **Enable DHCP server** checkbox, and enter the Start IP addresses, the End IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

7. Click **Next** to display the following screen.

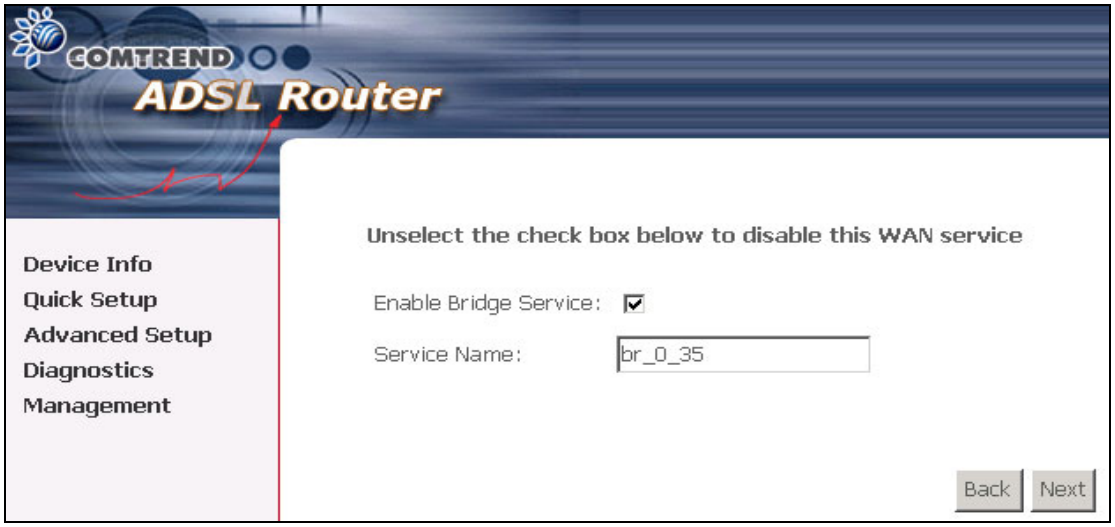


8. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5624 is ready for operation and the LEDs display as described in the LED description tables.

6.2.4 Bridging

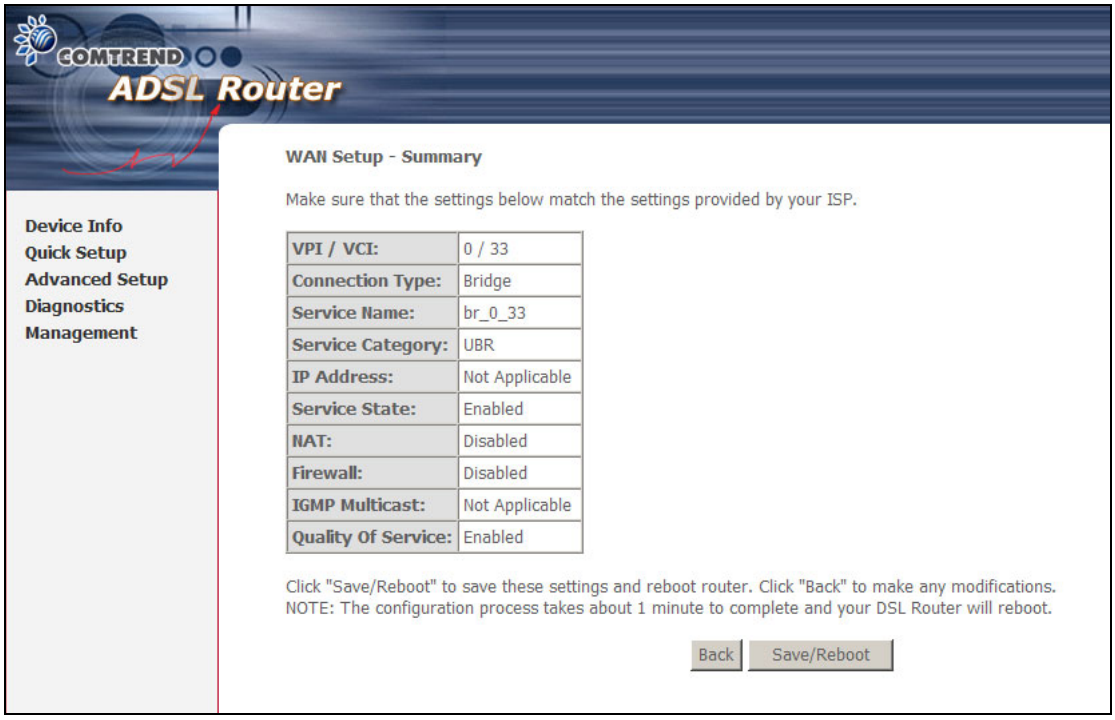
Select the bridging mode. To configure Bridging, do the following.

1. Select Quick Setup and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type in the VPI and VCI values provided by the ISP and click Next.
4. Select the Bridging radio button and click **Next**. The following screen appears. To use the bridge service, tick the checkbox, Enable Bridge Service, and enter the service name.



5. Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the ADSL router. Notice that there is no IP address for the WAN interface in bridge mode, and the remote technical support cannot access the ADSL router.

6. The following screen will be displayed.



The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

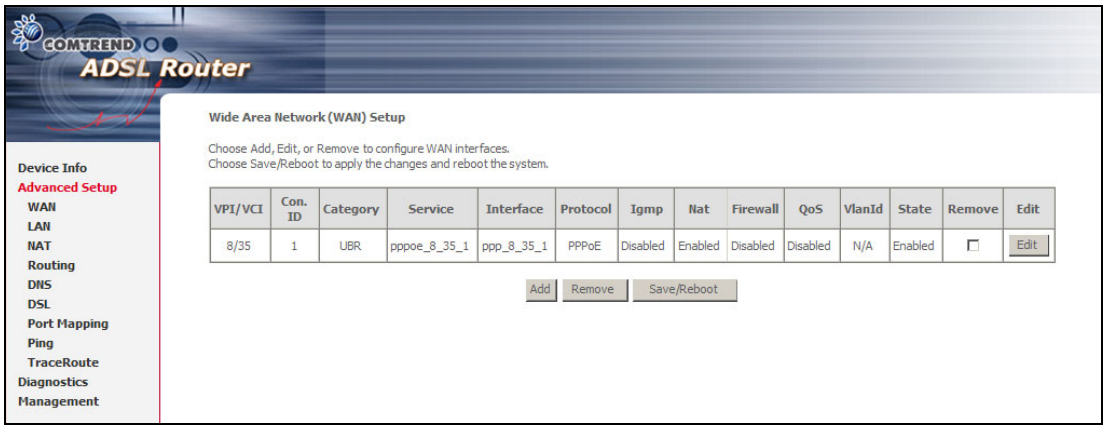
Chapter 7 Advanced Setup

This chapter includes the following sections:

WAN, LAN, NAT, Security, QoS, Routing, DNS, DSL, and Port Mapping

7.1 WAN

This screen shows the default WAN interface. Users can choose to **Add**, **Edit**, or **Remove** these WAN interfaces. The **Save/Reboot** button saves the current configuration and reboots the router.

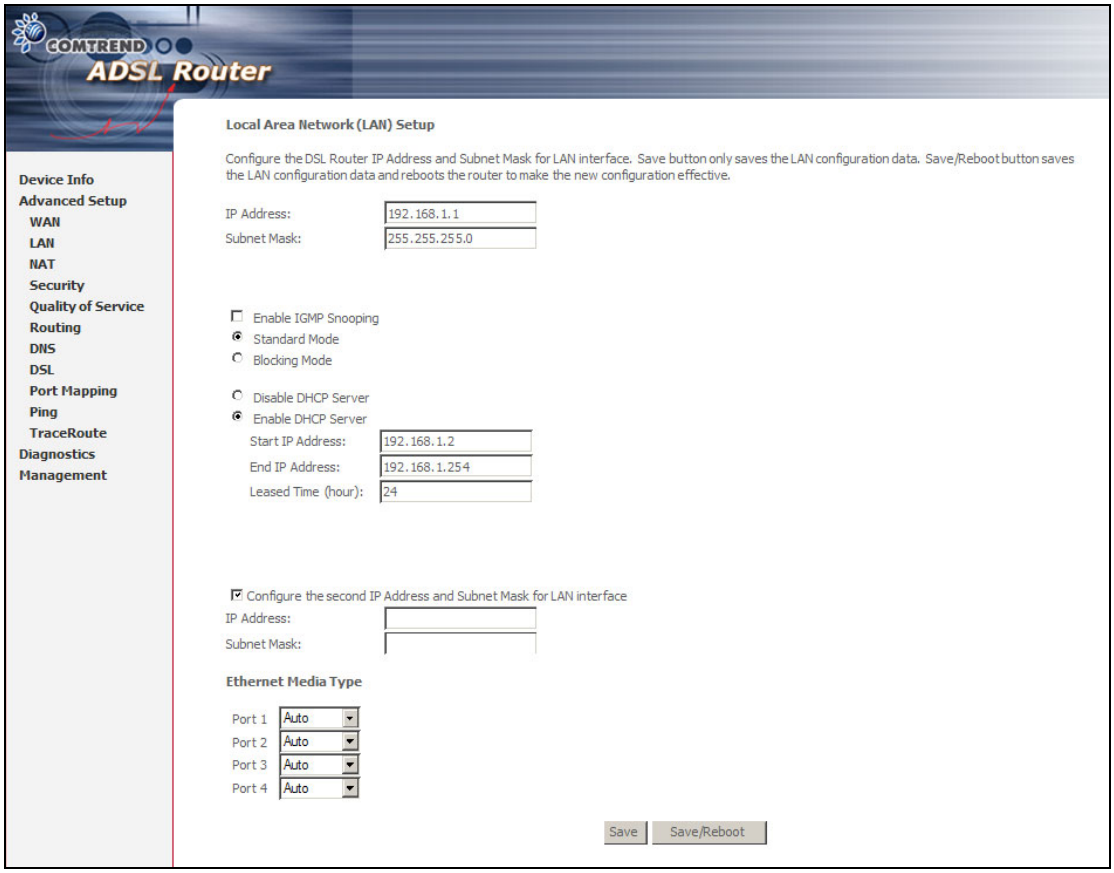


VlanID	This function means one can add an 802.1Q VLAN tag on PPPoE/MER or Bridge mode. It means the packets are sent to WAN and a specific VlanID (802.1Q tag) will be added in the Ethernet header. The VlanID shows which 802.1Q tag will be added.

For further information consult the table in section 5.1 WAN.

7.2 LAN

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.



IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable IGMP Snooping: Enable by ticking the box.

Standard Mode**:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

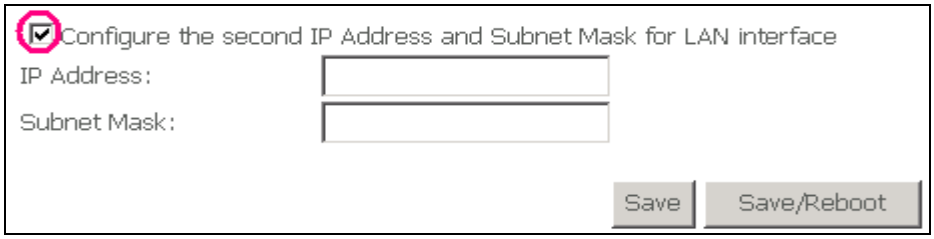
Blocking Mode**:** In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Configure the second IP address by ticking the checkbox shown below.

IP Address: Enter the secondary IP address for the LAN port.

Subnet Mask: Enter the secondary subnet mask for the LAN port.



NOTE:	The **Save** button saves new settings to allow continued configuration while the **Save/Reboot** button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

Ethernet Media Type: Choose Auto, 10_Half, 10_Full, 100_Half or 100_Full for each Ethernet port.

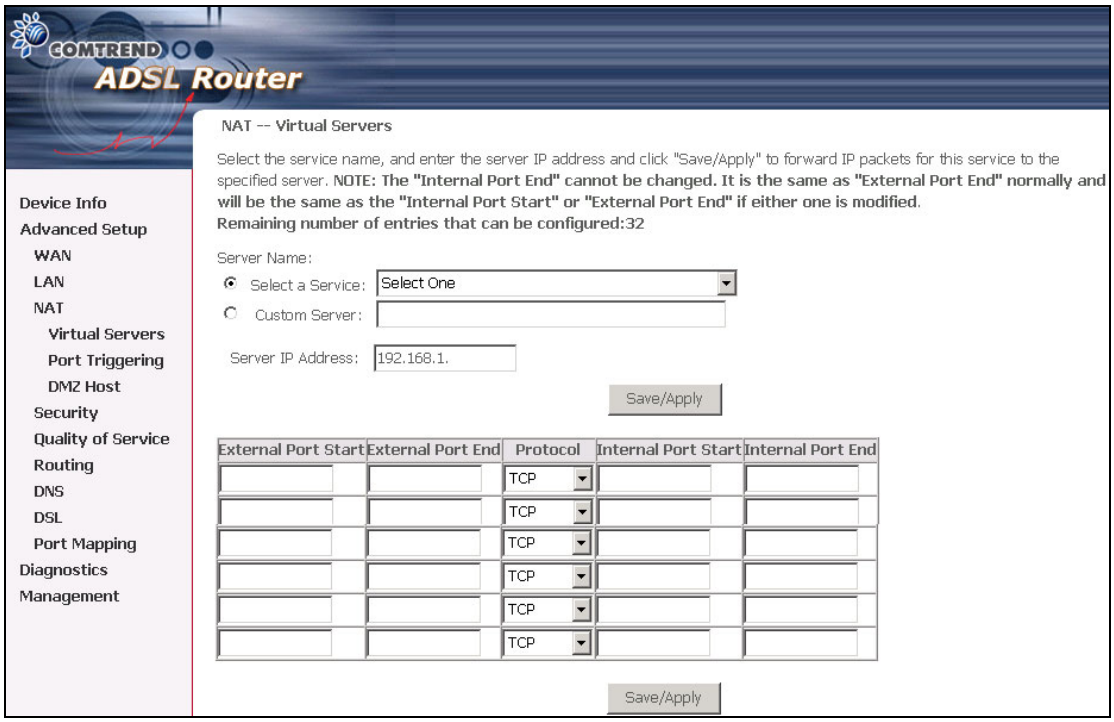
7.3 NAT

To display this function, you must enable NAT in WAN Setup.

7.3.1 Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

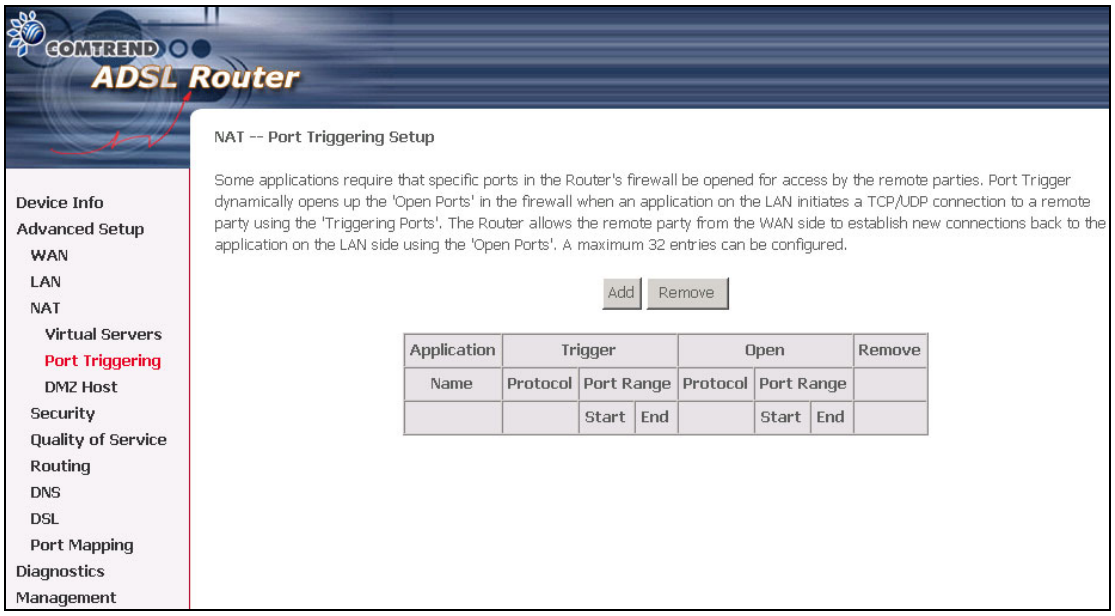
To add a Virtual Server, click the **Add** button. The following will be displayed.



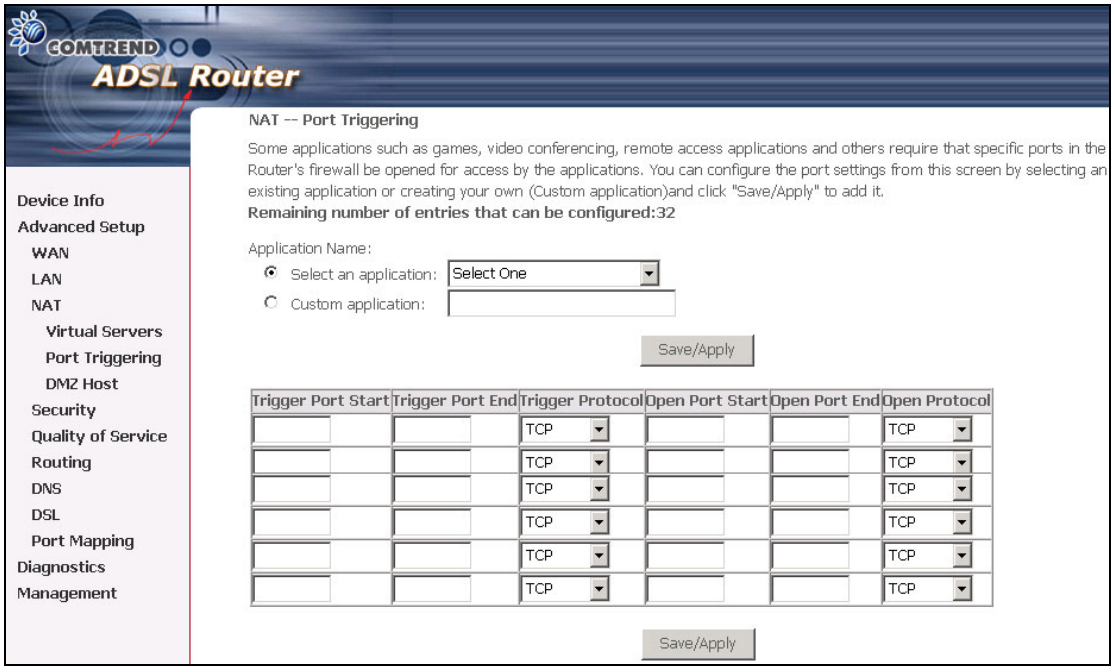
Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

7.3.2 Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

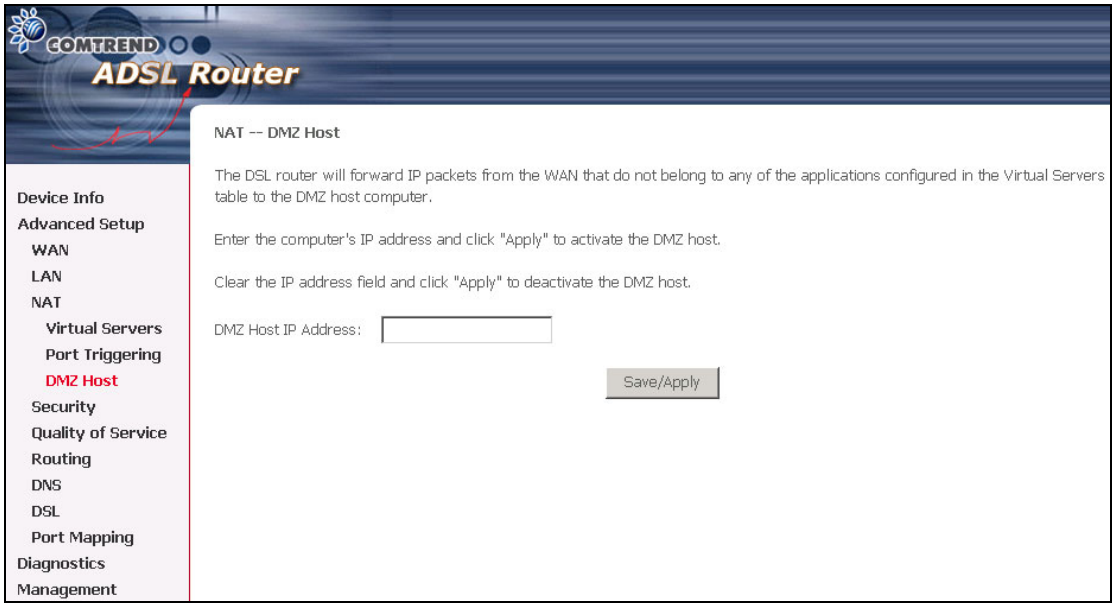


To add a Trigger Port, simply click the Add button. The following will be displayed.



7.3.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.

Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

7.4 Security

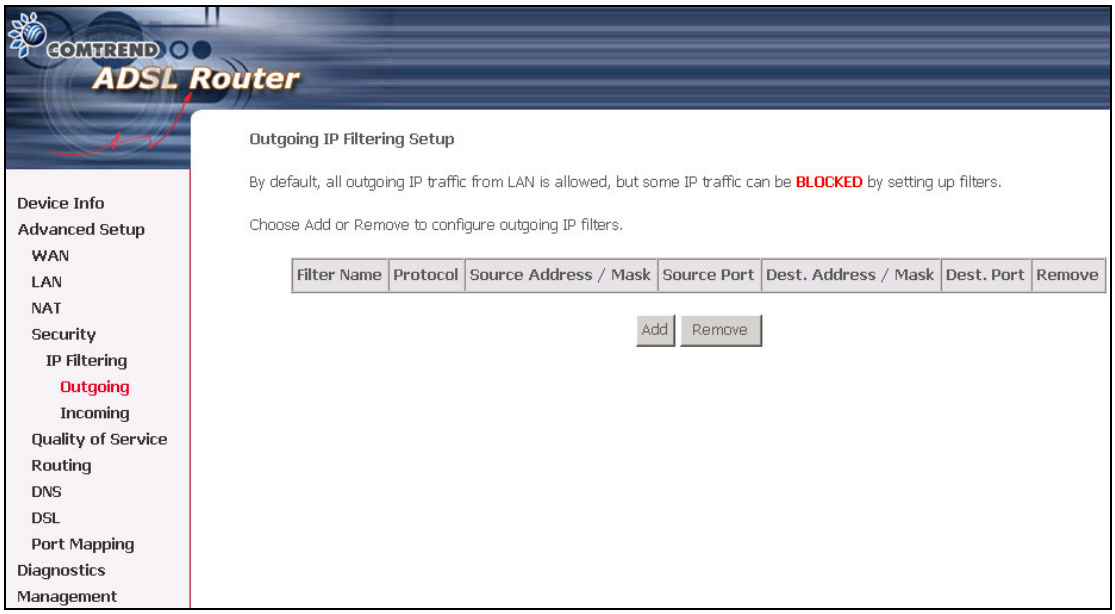
To display the Security function, you must enable the firewall in WAN Setup.

7.4.1 IP Filtering

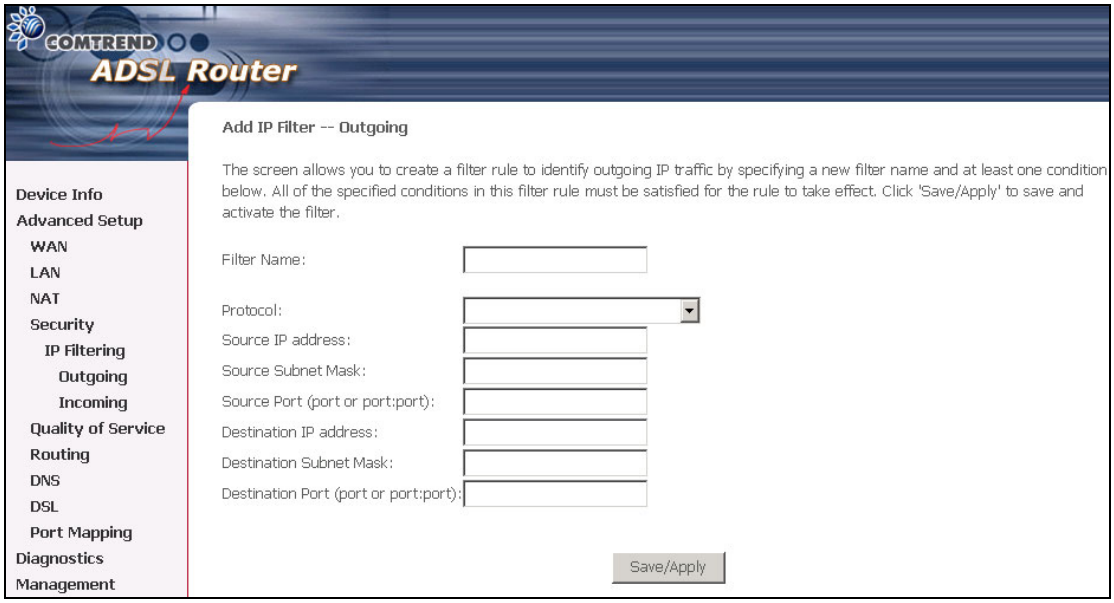
IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Outgoing

Note: The default setting for all Outgoing traffic is Accepted.



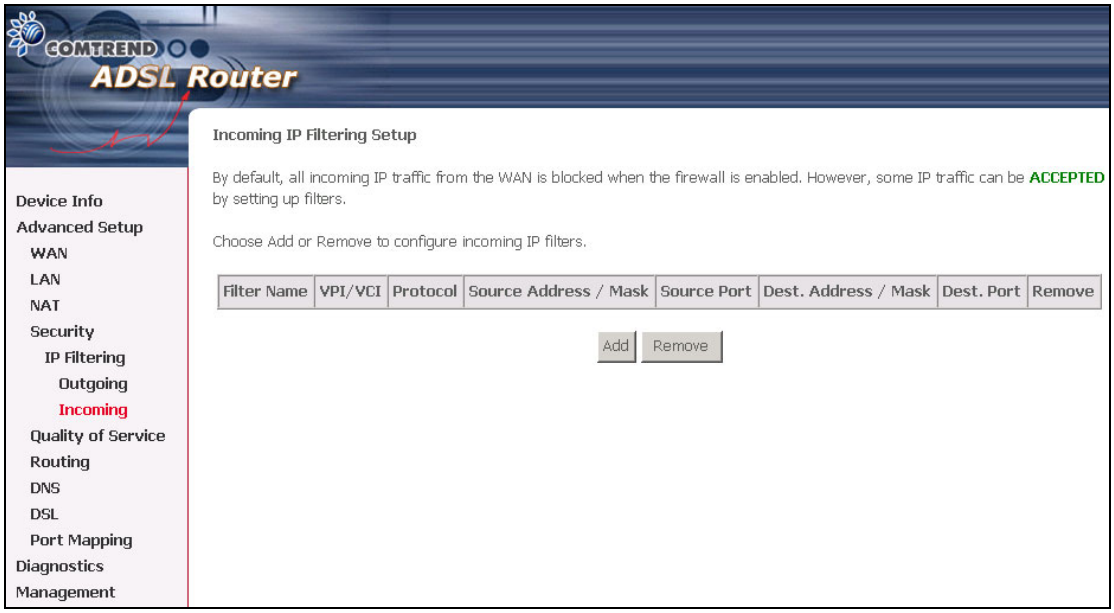
To add a filtering rule, simply click the Add button. The following screen will be displayed.



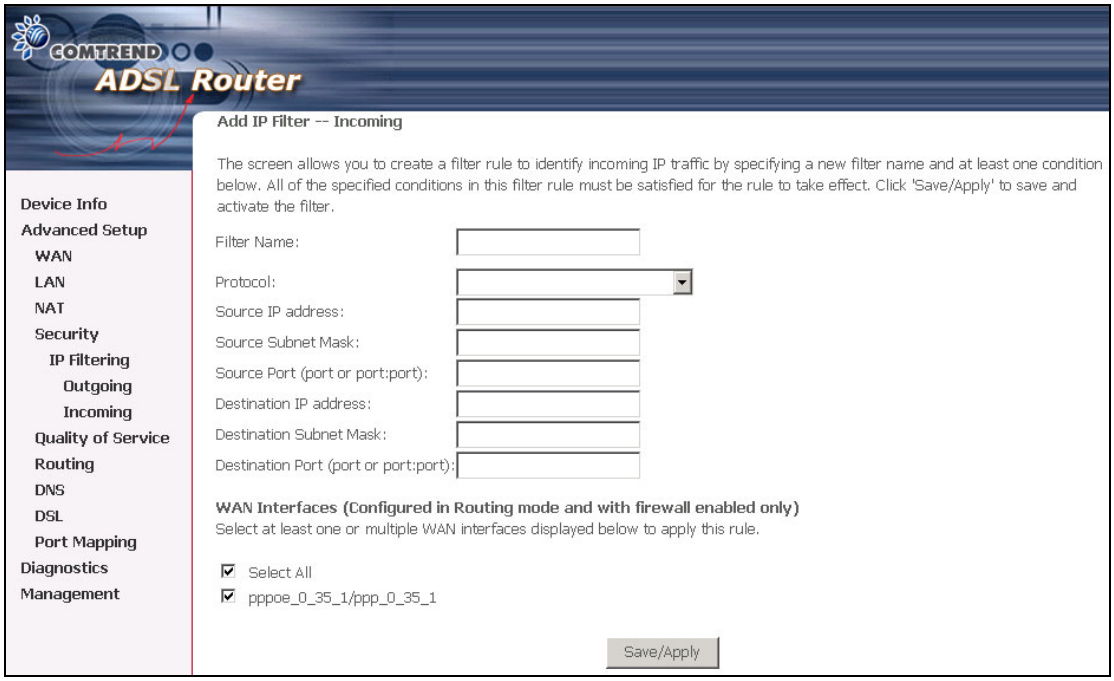
Filter Name	Type a name for the filter rule.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

Incoming

Note: The default setting for all Incoming traffic is Blocked.



To add a filtering rule, simply click the Add button. The following screen will be displayed.



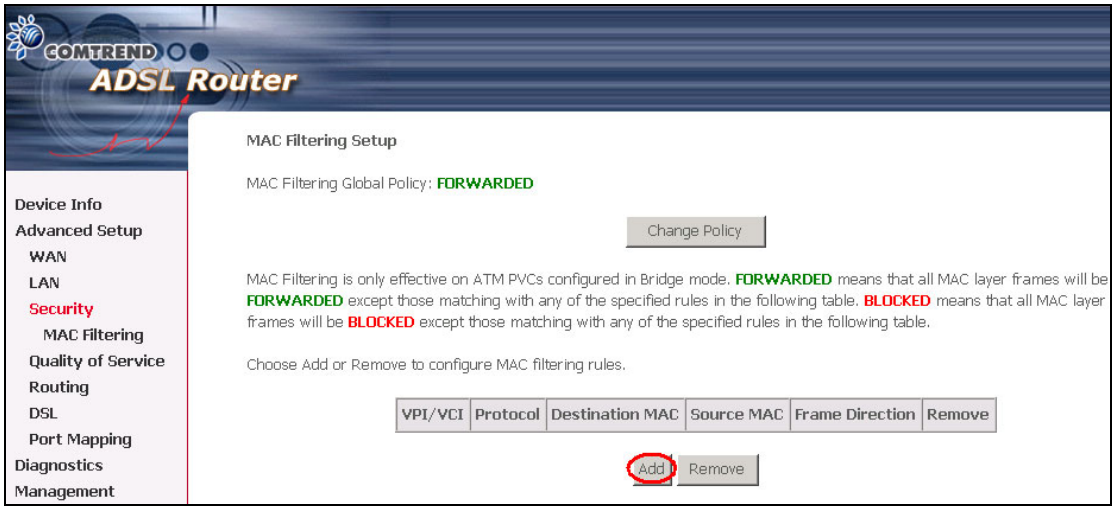
To configure the parameters, please reference **Outgoing** table above.

7.4.2 MAC Filter

NOTE:	This function is only available when in bridge mode. PPPoE, PPPoA, IPoA and MER use IP Filtering (pg. 43) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the CT-5624 can be set according to the following procedure.

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the rules specified in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the rules specified in the following table. The default policy is **FORWARDED**. This can be changed by clicking the **Change Policy** button.

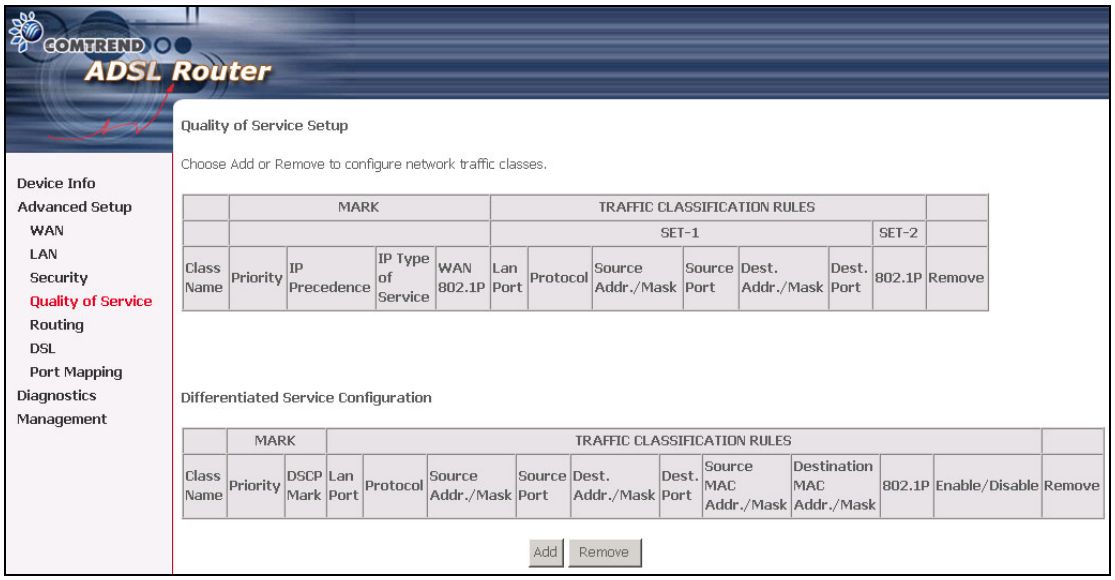


Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save/Apply** to save and activate the filter rule.

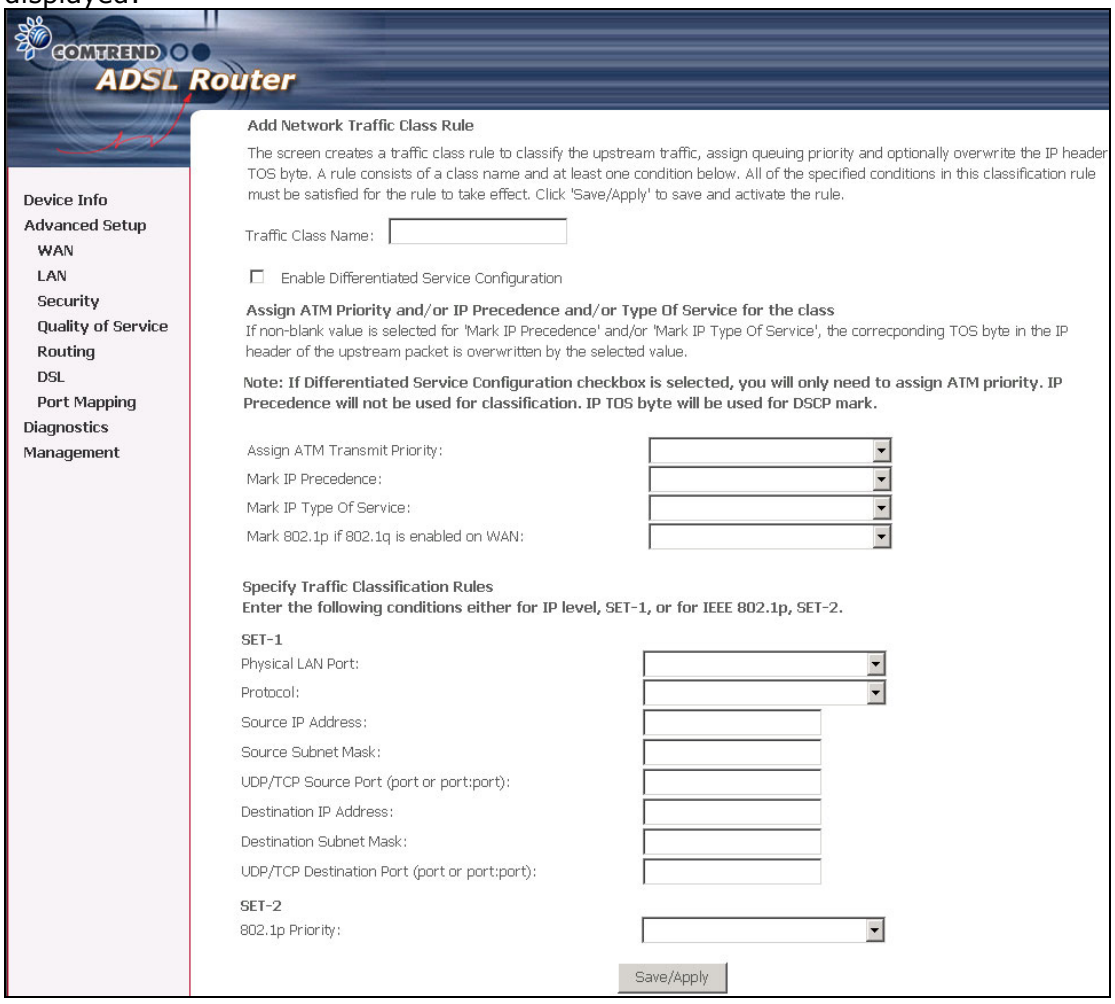
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies filter to selected PVCs (bridge mode only). Filter rules are arranged according to PVC, as shown under the VPI/VCI heading on the previous screen.

7.5 Quality of Service

To display this function, you must enable QoS in WAN Setup.



Choose **Add** to configure network traffic classes. The following screen will be displayed:



The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.	
Traffic Class Name	Enter name for traffic class
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit shows the higher the priority If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value. **Note:** If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value. **Note:** If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign Differentiated Services Code Point (DSCP) Mark	Choose the required DSCP value. Default value is “000000”.
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7.
Specify Traffic Classification Rules Enter the following conditions either for physical LAN port or for IP level, SET-1, or for IEEE 802.1p, SET-2	
SET-1	
Physical LAN Port	User can select from: ENET, ENET(1-4).
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.

Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
SET-2	
802.1p Priority	Select between 0-7.
Traffic Class Name	Enter name for traffic class
Priority	Select Low, Medium or High.
IP Precedence	Select between 0-7. The lower the digit shows the higher the priority
IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Physical LAN Port	User can select from: ENET, ENET(1-4).
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

7.6 Routing

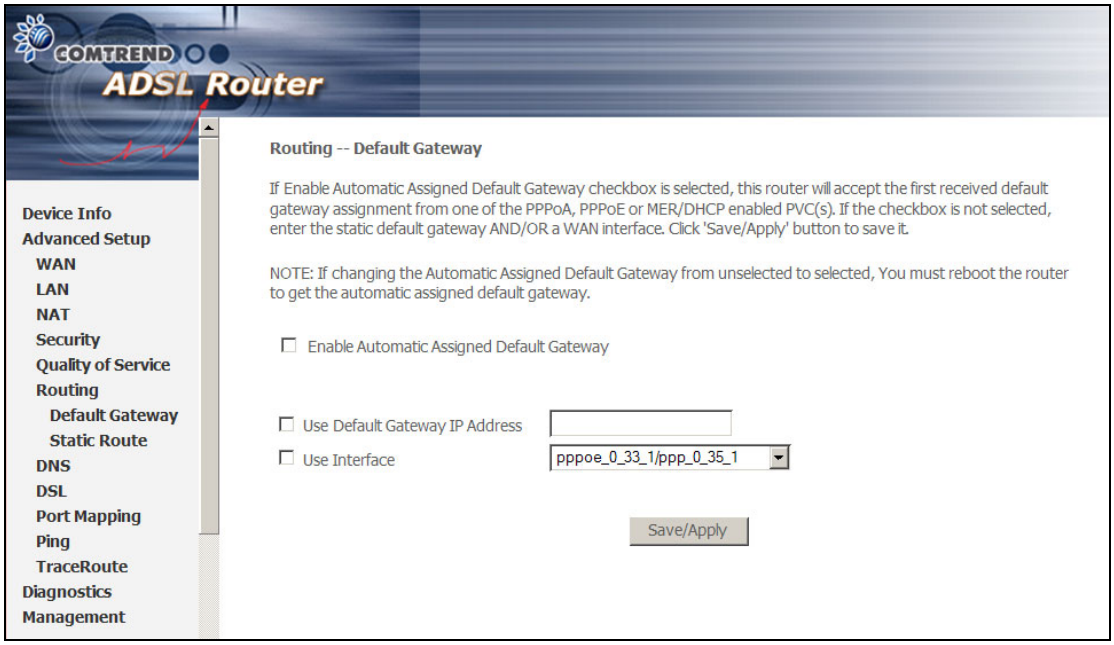
The Routing dialog box allows you to configure Default Gateway and Static Route.

7.6.1 Default Gateway

If '**Enable Automatic Assigned Default Gateway'** checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s).

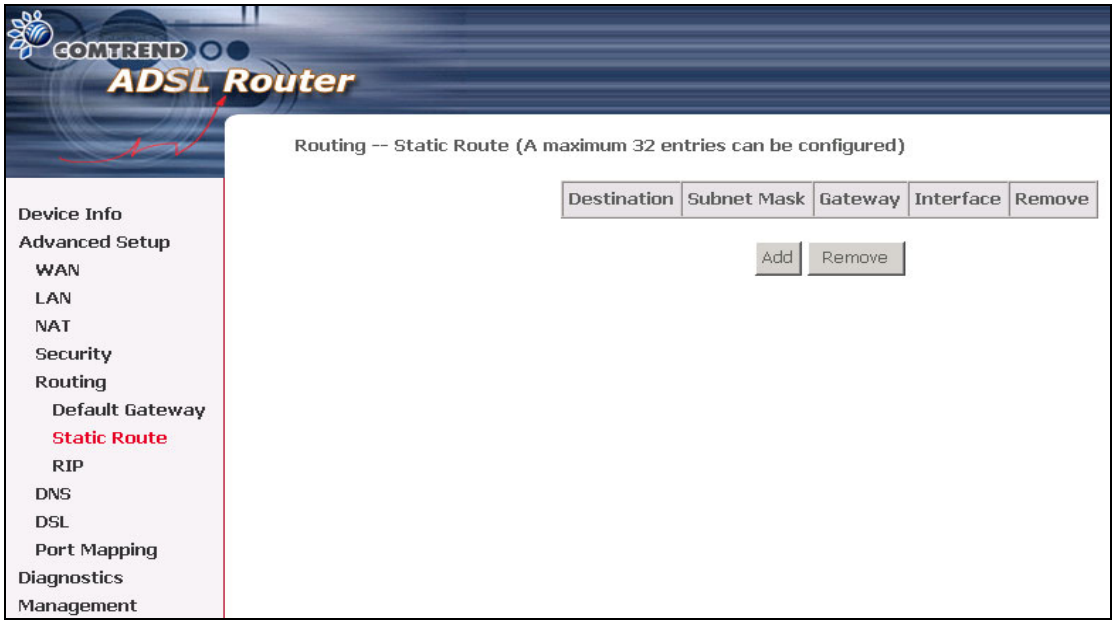
If the checkbox is not selected (as shown below), enter the static default gateway AND/OR a WAN interface, then click **Save/Apply**.

NOTE:	When enabling the Automatic Assigned Default Gateway, you must reboot the router to receive the default gateway IP address.

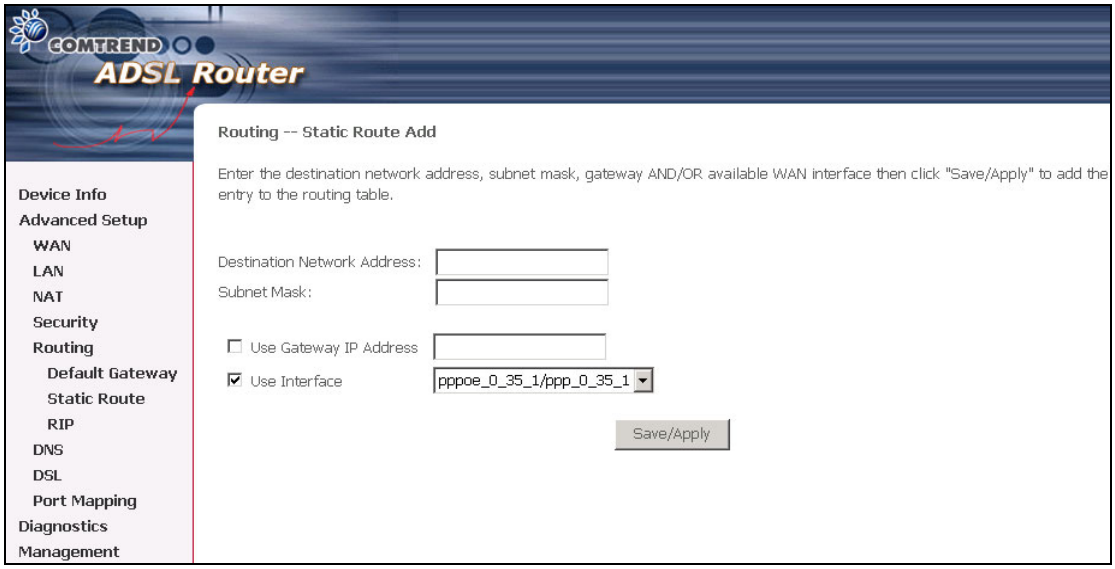


7.6.2 Static Route

Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.

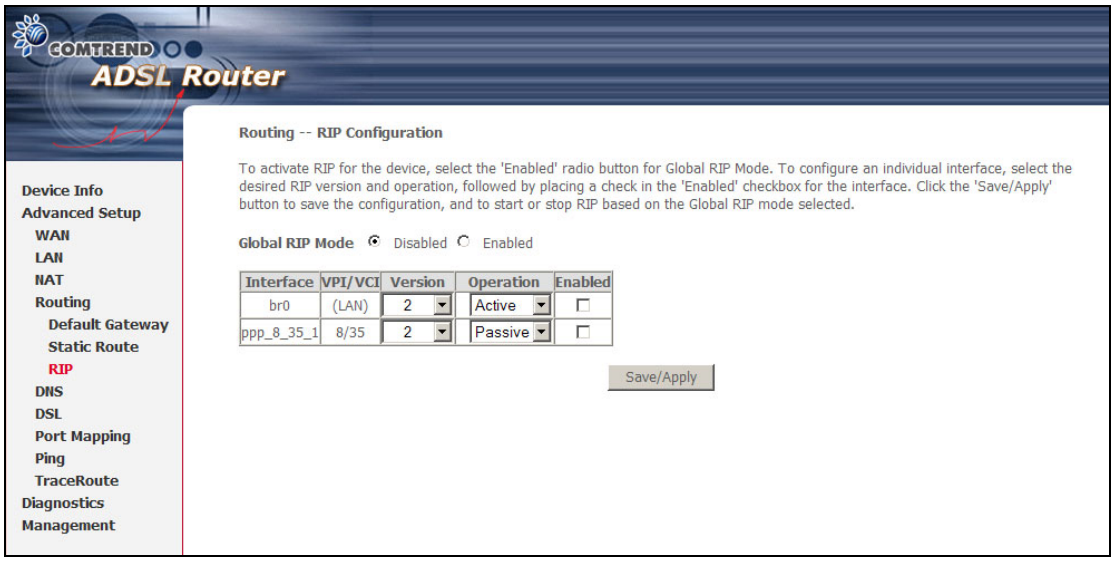


To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway and available WAN interface then click **Save/Apply** to add the entry to the routing table.



7.6.3 RIP

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

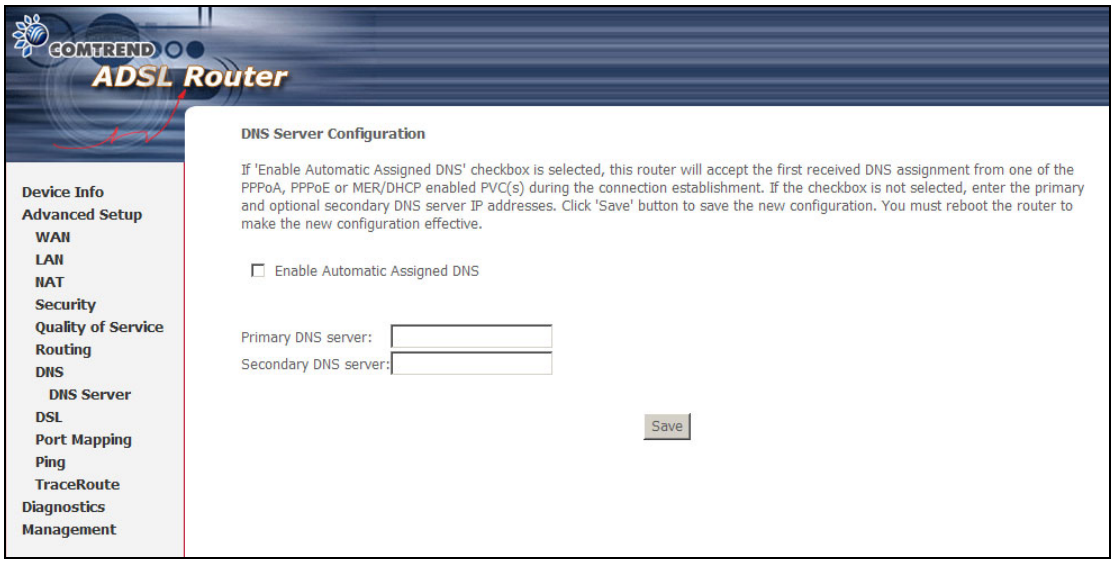


Note: This screenshot is based on PPPoE encapsulation.

7.7 DNS

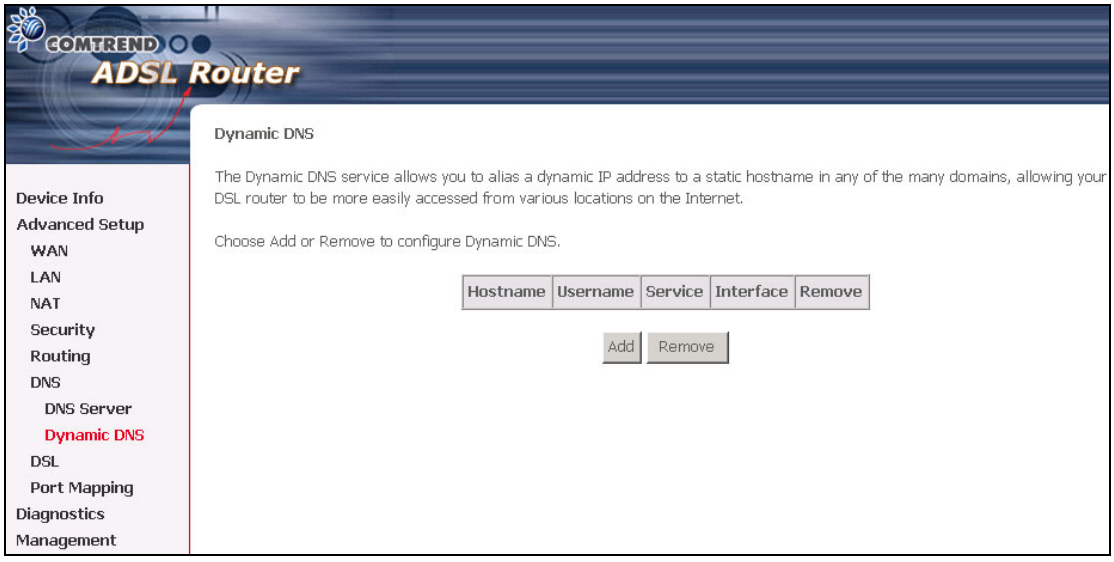
7.7.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.



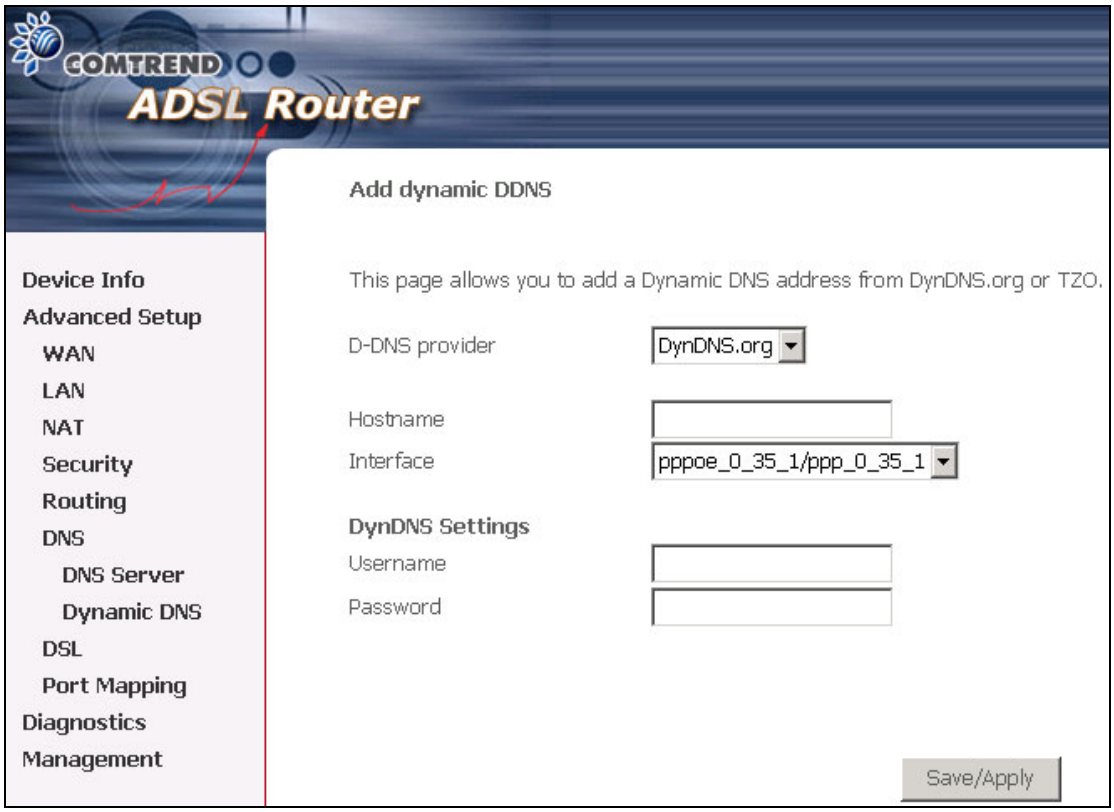
7.7.2 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.



NOTE:	The Add/Remove buttons will only be displayed if the CPE has already been assigned an IP address from the remote server.

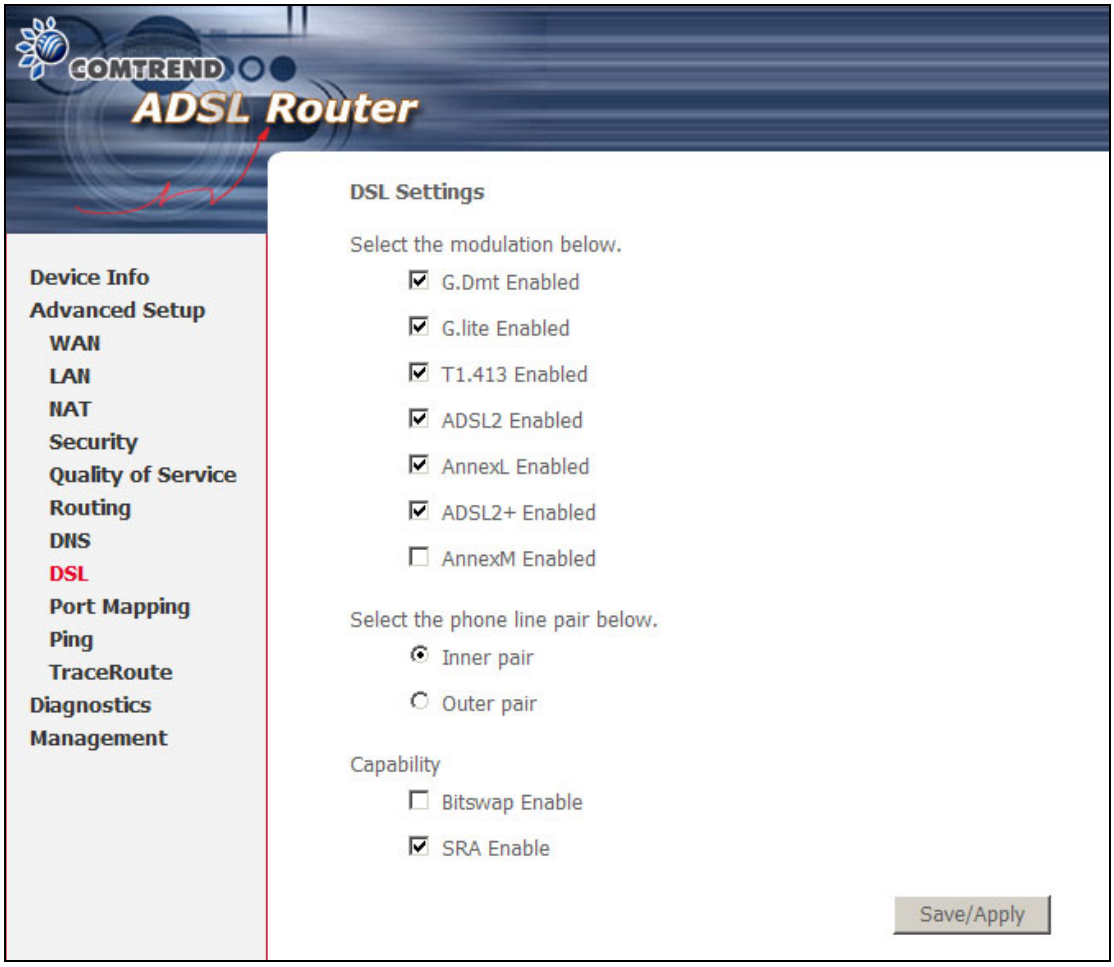
To add a dynamic DNS service, simply click the Add button. The following screen will be displayed:



D-DNS provider	Select a dynamic DNS provider from the list.
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list.
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

7.8 DSL

To access the DSL settings, first click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode.

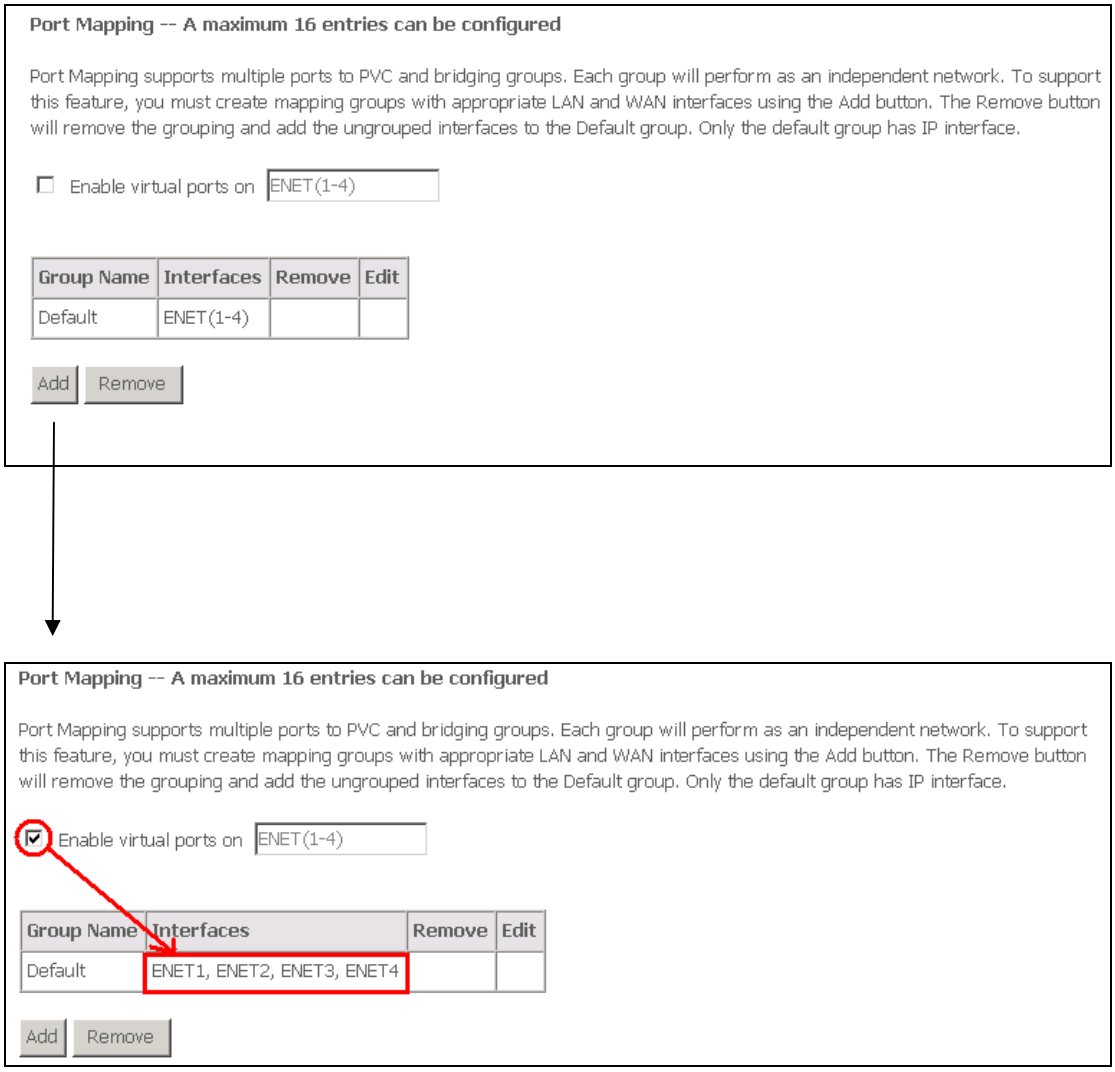


Option	Description
G.dmt Enabled	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite Enabled	Sets G.Lite if you want the system to use G.Lite mode.
T1.413 Enabled	Sets the T1.413 if you want the system to use only T1.413 mode.
ADSL2 Enabled	The device can support the functions of the ADSL2.
AnnexL Enabled	The device can support/enhance the long loop test.
ADSL2+ Enabled	The device can support the functions of the ADSL2+.
AnnexM Enabled	Covers a higher "upstream" data rate version, by making use of some of the downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswapping function.
SRA Enable	Allows seamless rate adaptation.

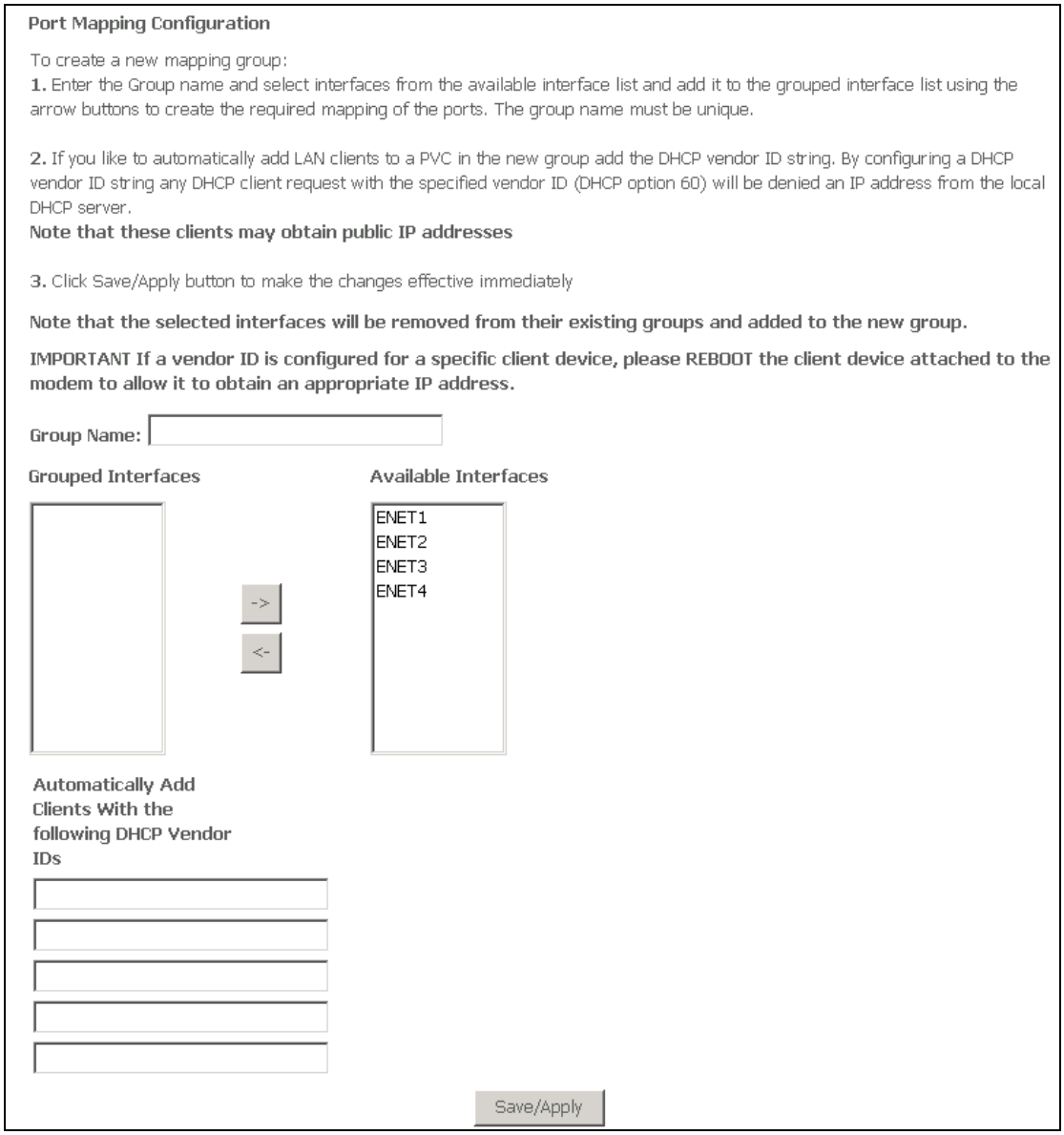
7.9 Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.



To add a port mapping group, simply click the **Add** button.



To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Automatically Add Clients With the Following DHCP Vendor IDs:
Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Port Mapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video). The Lan interfaces are ETH1, ETH2, ETH3 and ETH4.

Port mapping configuration are:

1. Default : ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

The CPE's dhcp server is running on "Default". And ISP's dhcp server is running on PVC 0/36. It is for setup-box use only.

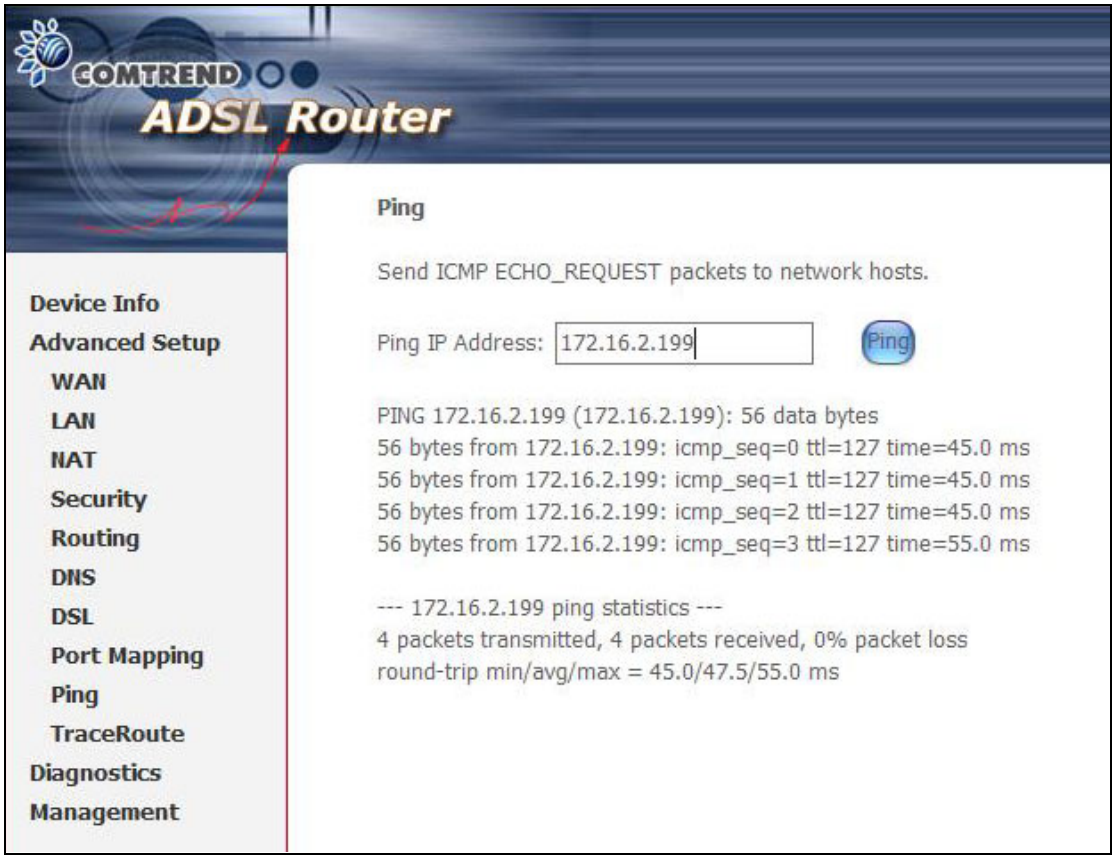
In the LAN side, PC can get IP address from CPE's dhcp server and access Internet via PPPoE (0/33).

If the setup-box was connected with interface "ENET1" and send a dhcp request with vendor id "Video", CPE's dhcp server will forward this request to ISP's dhcp server.
And CPE will change the port mapping configuration automatically. The portmapping configuration will become:

1. Default : ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, nas_0_38 and ENET1.

7.10 Ping

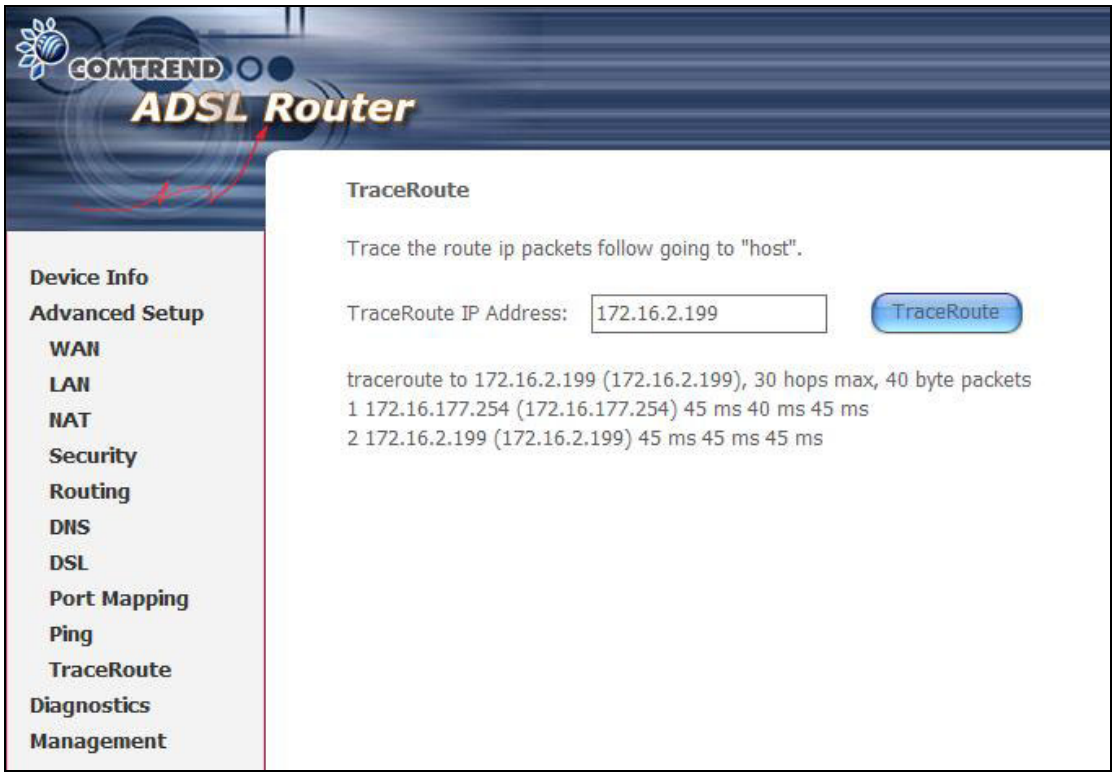
This screen performs the same function as the console command of the same name. It allows you to check the connection between the router and any location on the LAN or WAN. Enter the IP address of the location you wish to check and click **Ping**. The router will "ping" the IP address four times, as shown in the figure below.



NOTE: In the example above, all four data packets were transmitted successfully, resulting in 0% packet loss. This indicates a good connection. By comparison, a poor connection will have some packet loss and no connection will result in 100% packet loss.

7.11 TraceRoute

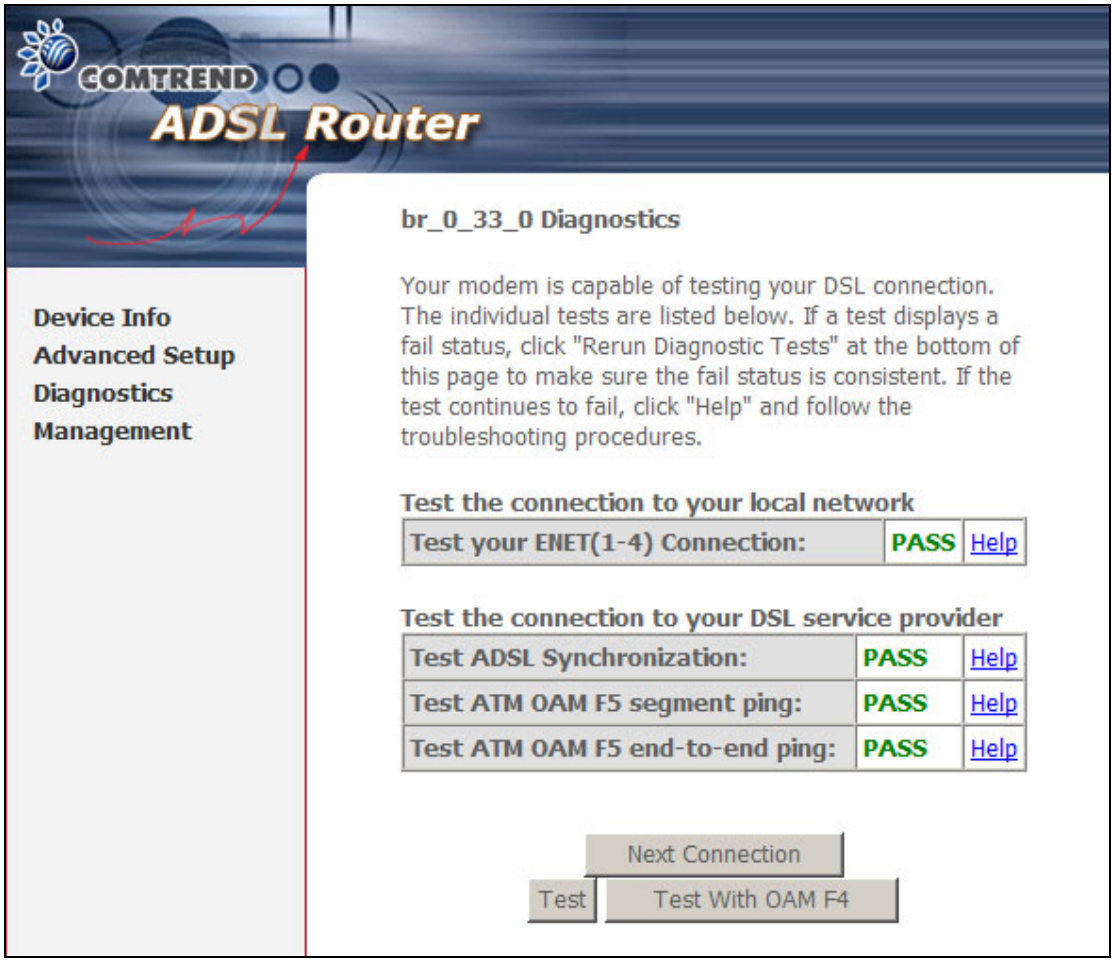
This screen performs the same function as the console command of the same name. It allows you to trace the path between the router and any location on the LAN or WAN within 30 hops of the router. Enter the IP address of the location you wish to trace and click **TraceRoute.**



NOTE: In the example above, the final IP address listed is the target IP address (i.e. 172.16.2.199). If the target IP address does not appear at the end of this list, **ping** the target IP address to test the connection.

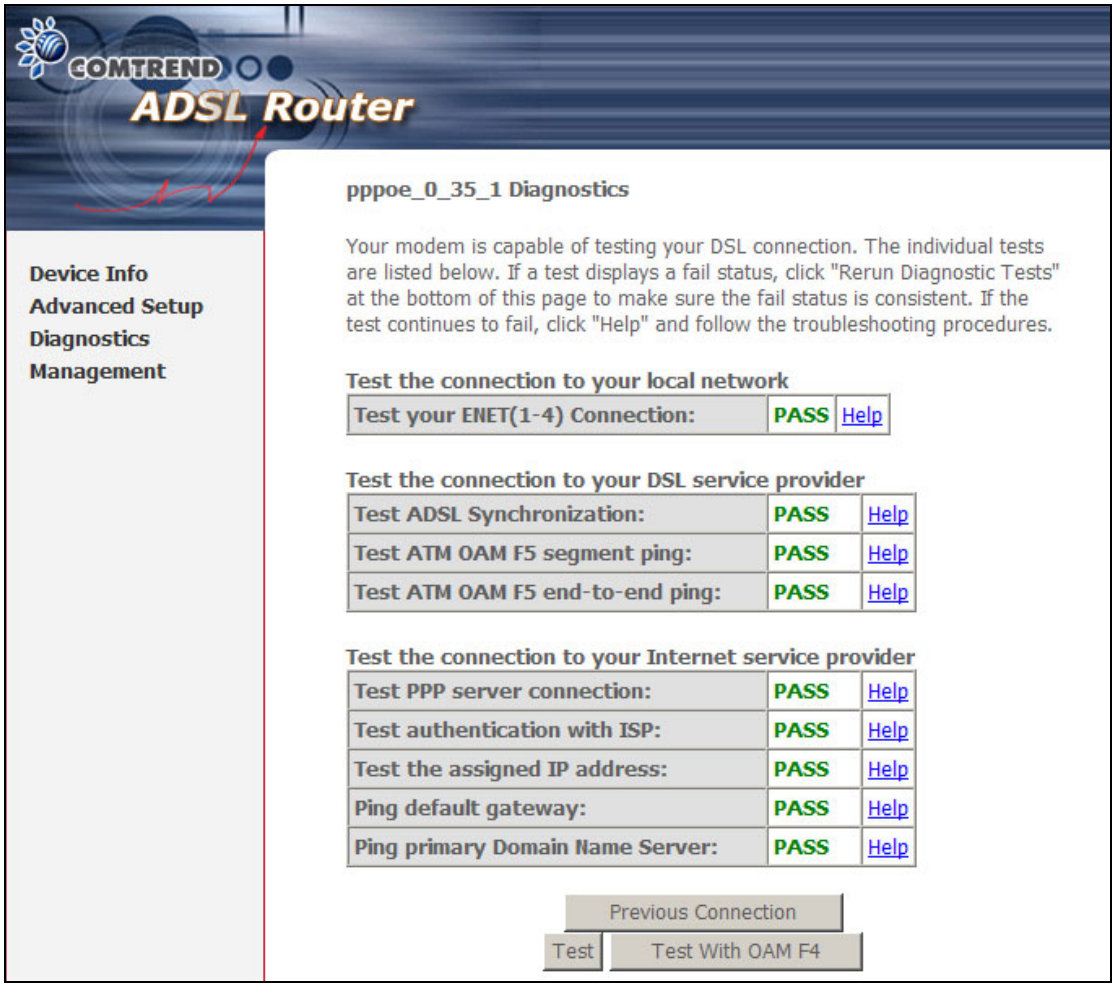
Chapter 8 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-5624 and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



Test	Description
Ethernet Connection	**Pass:** Indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. **Fail:** Indicates that the DSL Router does not detect the Ethernet interface on your computer.
ADSL Synchronization	**Pass:** Indicates that the DSL modem has detected a DSL signal from the telephone company. **Fail:** Indicates that the DSL modem does not detect a signal from the telephone company's DSL network.

In router modes, such as PPPoE, this screen will also include ISP tests as shown.



ISP Connection	**Pass:** Indicates that the router can access the ISP Default Gateway or Domain Name Server (DNS). **Fail:** Indicates that the router cannot access the ISP Default Gateway or Domain Name Server (DNS).

Chapter 9 Management

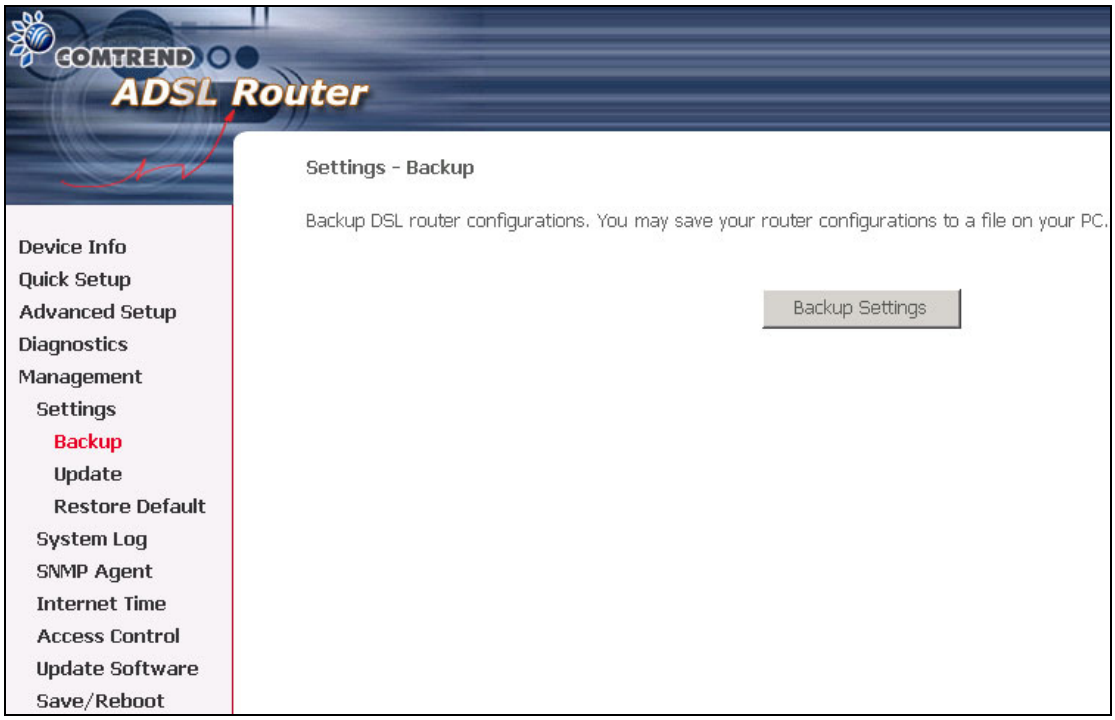
The system administrator can do the following functions to manage the configurations, events, SNMP information, user accounts, and software update of the CT-5624.

9.1 Settings

The Settings option allows you to back up your settings to a file and retrieve the file settings. The settings can be saved from ATUR to PC. The saved setting file can also be loaded from PC to ATUR. These 2 functions can help the system administrator to manage large amount of ATURs efficiently. Restore Default would set the ATUR with the factory default configuration.

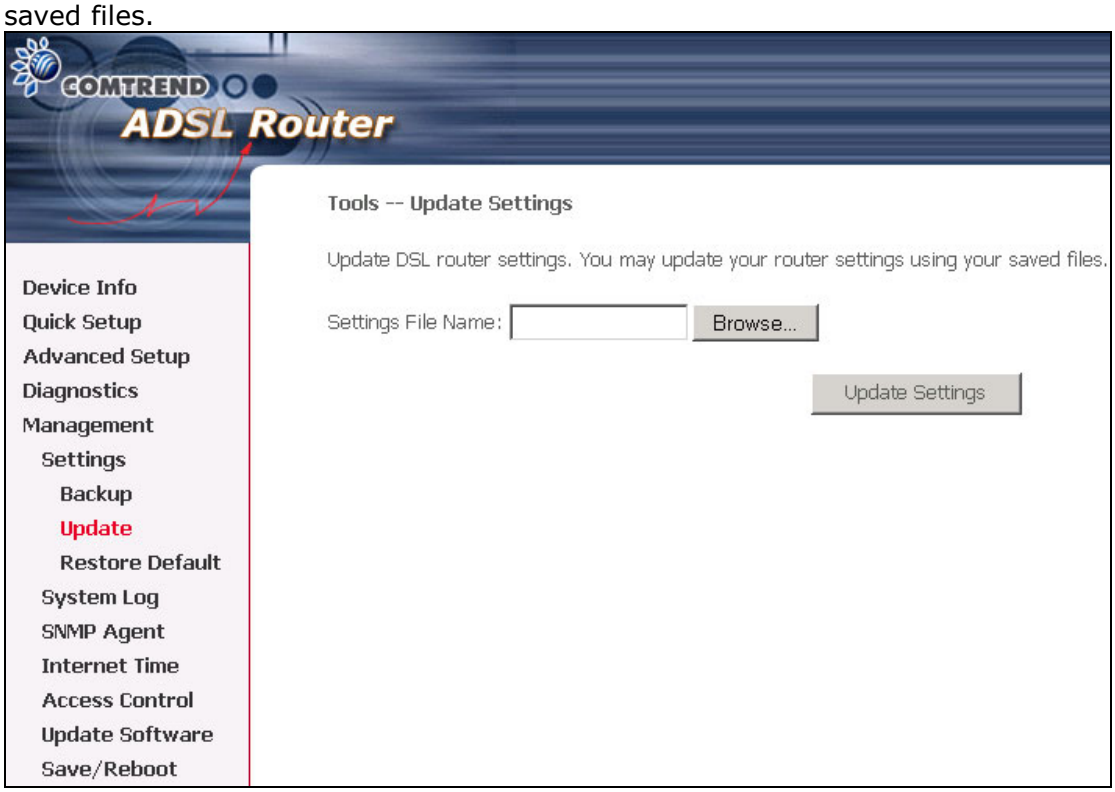
9.1.1 Backup Settings

The Backup option under Management>Settings save your router configurations to a file on your PC. Click BACKUP Settings in the main window. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings.** Te file will then be saved to the assigned location.



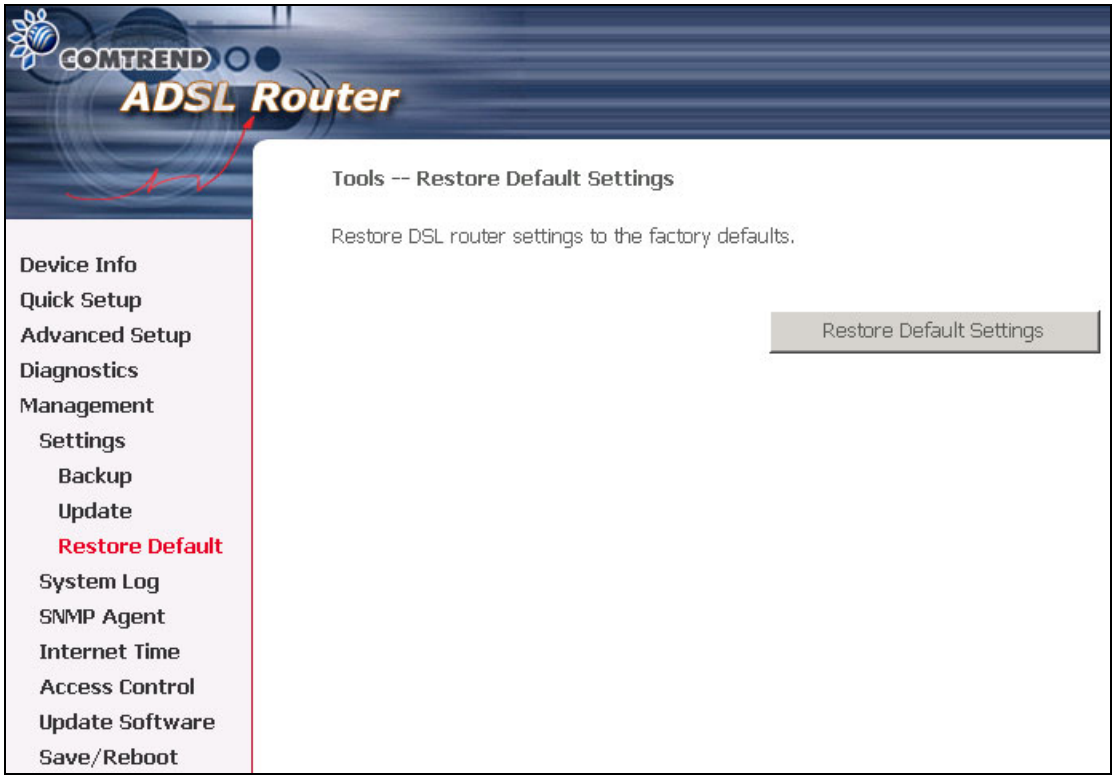
9.1.2 Update Settings

This option under Management>Settings updates your router settings using your saved files.



9.1.3 Restore Default

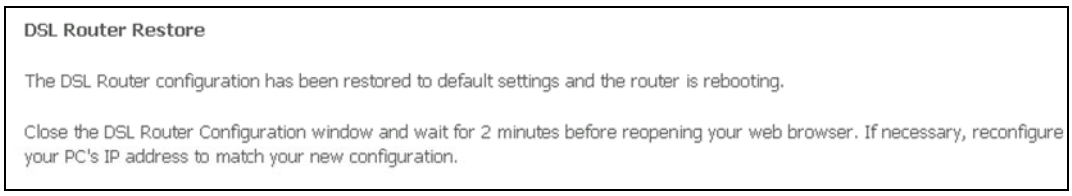
Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings.



NOTE: This entry has the same effect as the hardware reset-to-default button. The CT-5624 board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

NOTE: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-5624.

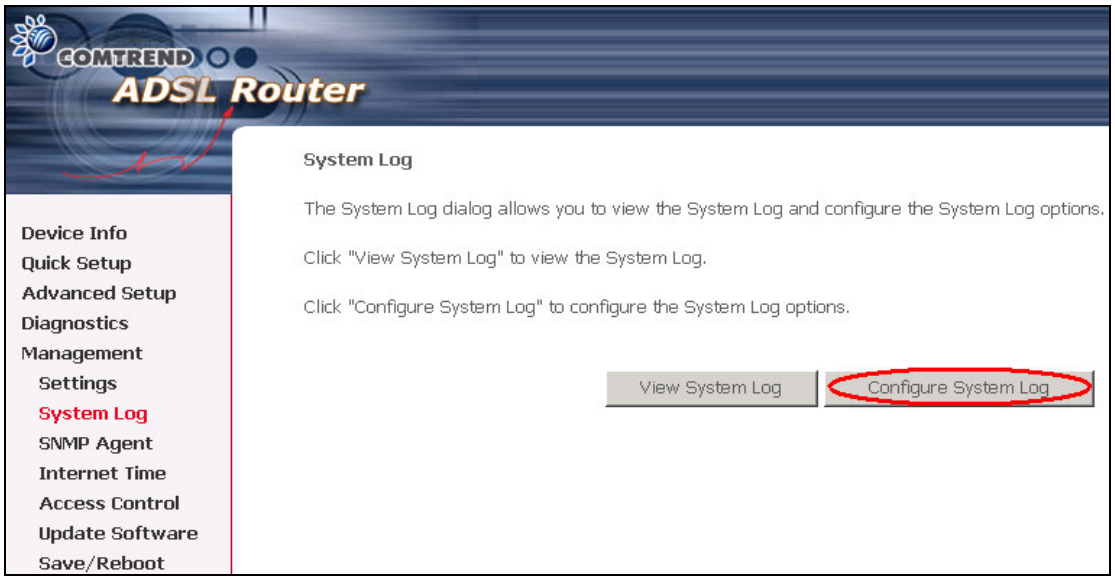
After the Restore Default Configuration button is selected, the following screen appears. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



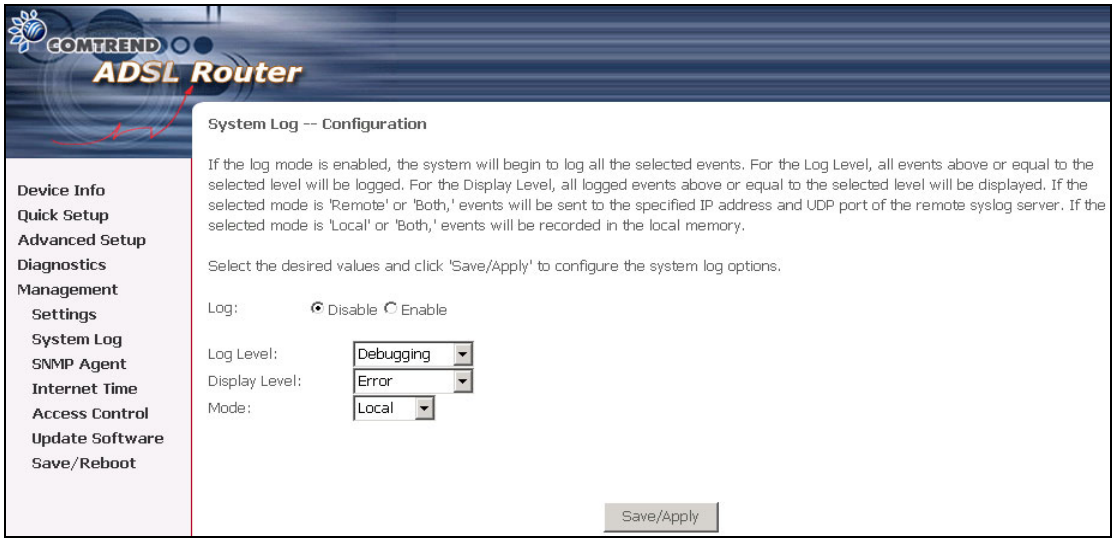
9.2 System Log

The System Log option under Management>Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1. Click **Configure System Log** to display the following screen.

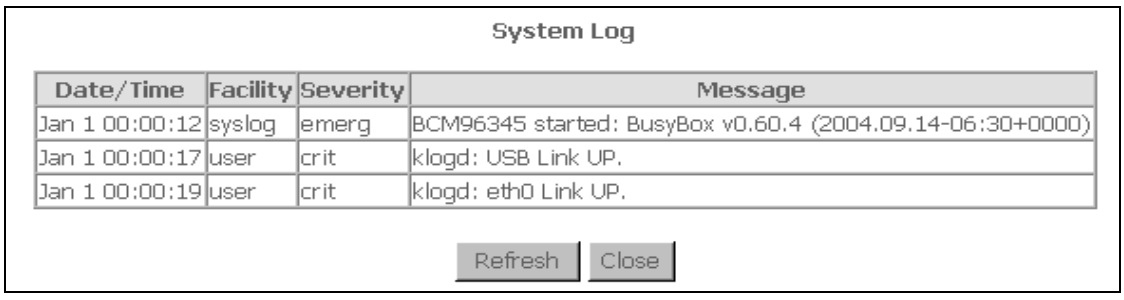


2. Select from the desired Log options described in the following table, and then click **SAVE/Apply**.



Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5624 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** page for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

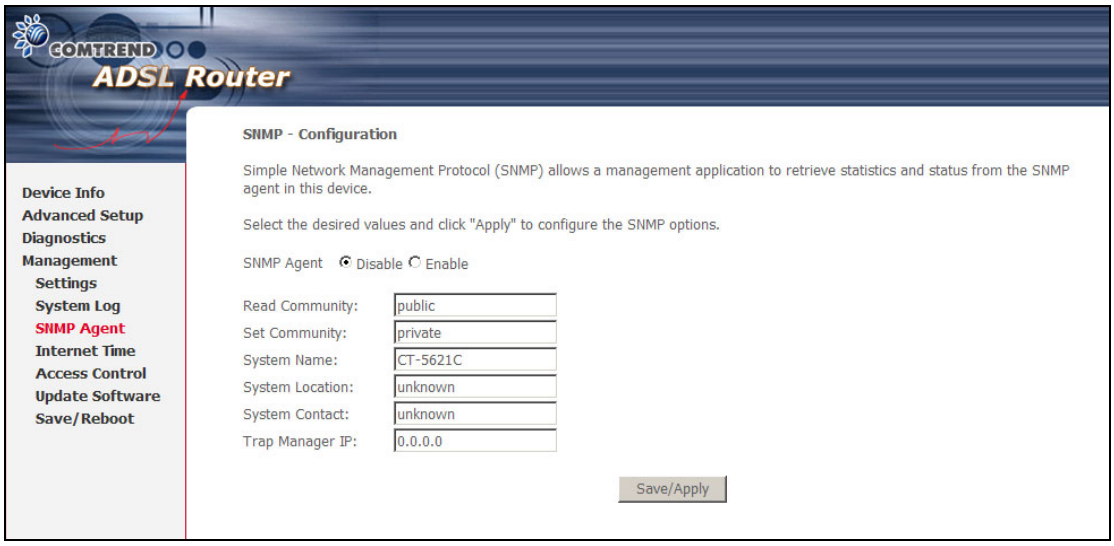
3. Click **View System Log**. The results are displayed as follows.



9.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select desired settings and click **Save/Apply** to apply changes.



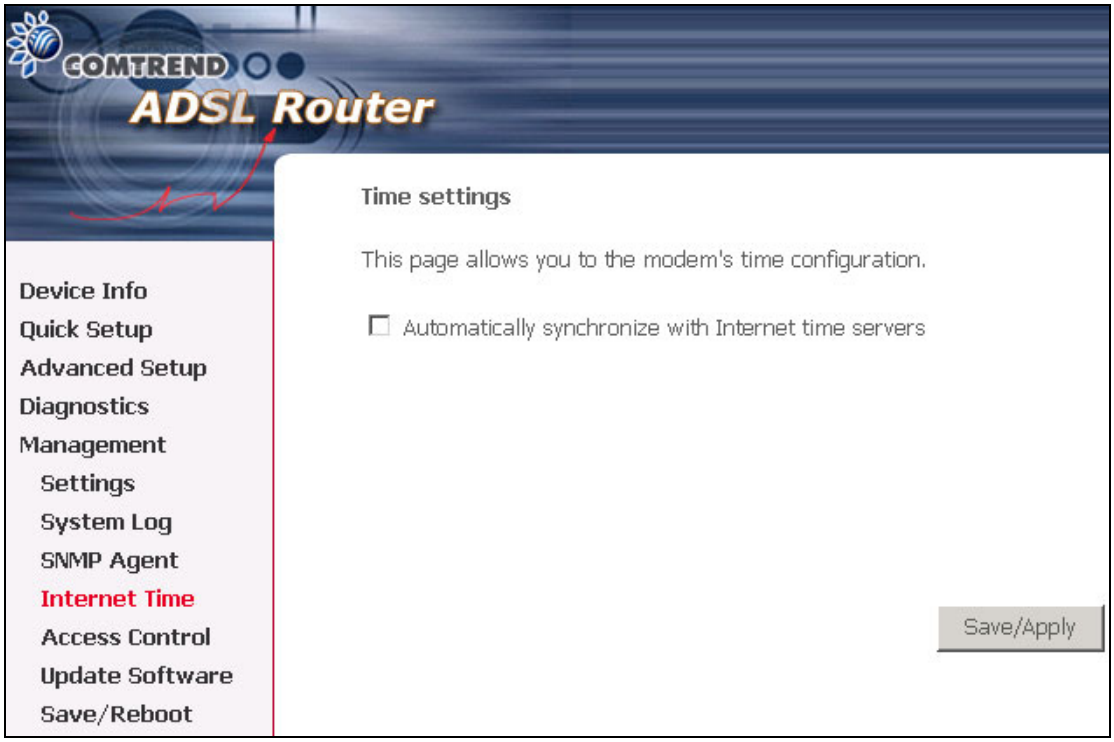
Enable or Disable the SNMP Agent.

Relationship between an Agent and Managers

Read Community:	Default is "public"
Set Community:	Default is "private"
System Name:	Default is "Comtrend"
System Location:	Shows the location of the system.
System Contact:	Shows the who should be contacted about the host the agent is running on.
Trap Manager IP:	Trap request supports to monitor and alarm via port 162 from Agent.

9.4 Internet Time

The Internet Time option under Management menu bar configures the Modem's time. To automatically synchronize with Internet time servers, tick the corresponding box displayed on the screen. Then click **Save/Apply**.

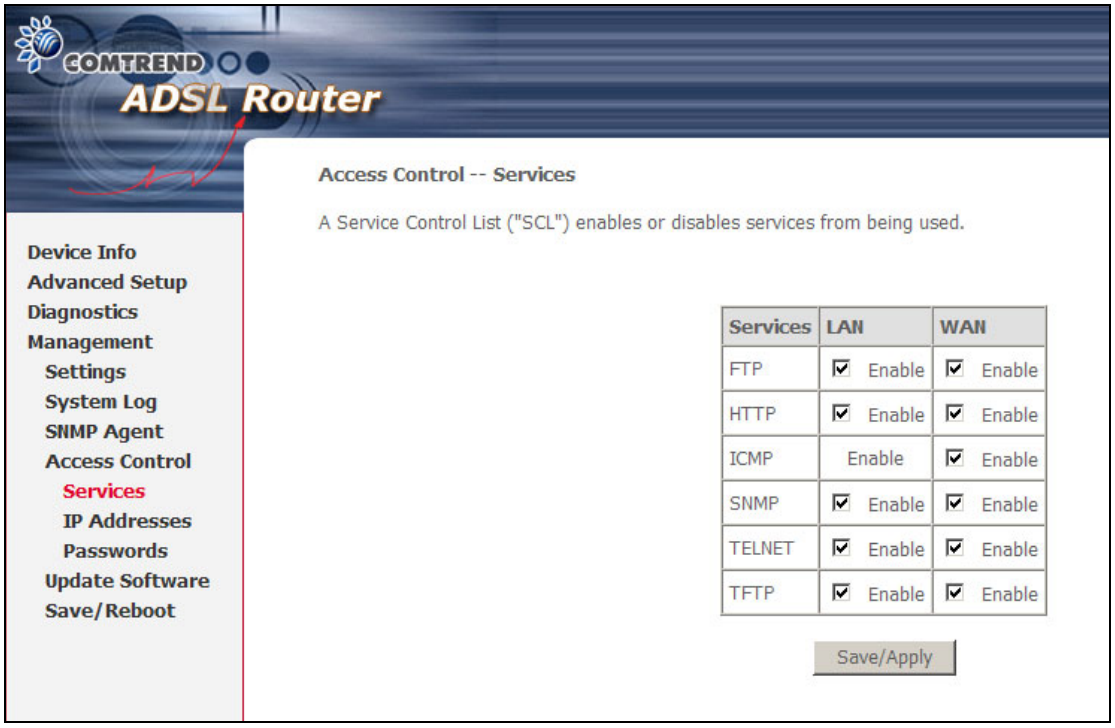


9.5 Access Control

The Access Control option under Management menu bar configures the access-related parameters, including three parts: Services, IP Address, and Passwords.

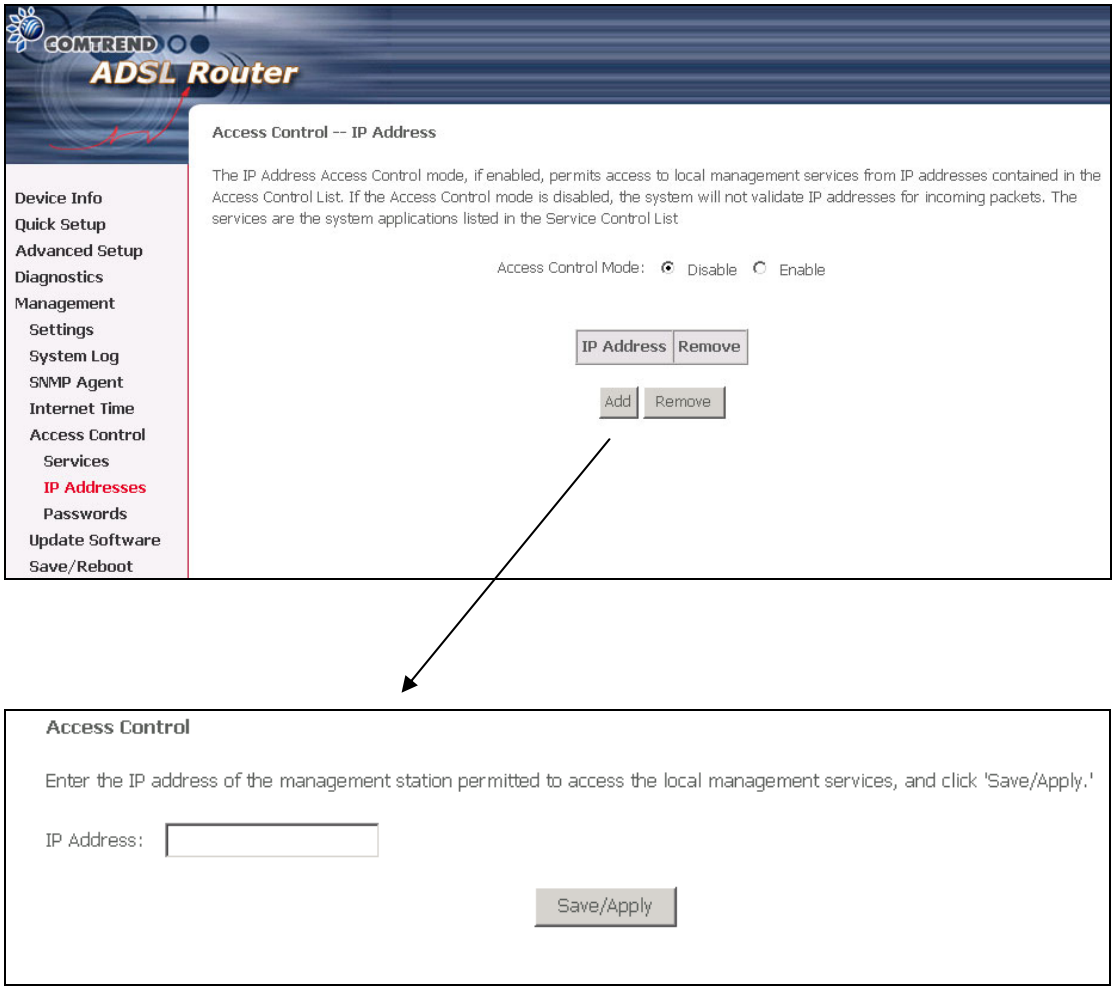
9.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SNMP, TELNET, and TFTP. The "Services" can be enabled for LAN side, WAN side, or both. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



9.5.2 IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the router. Before you enable it, configure the IP addresses by clicking the **Add** button.



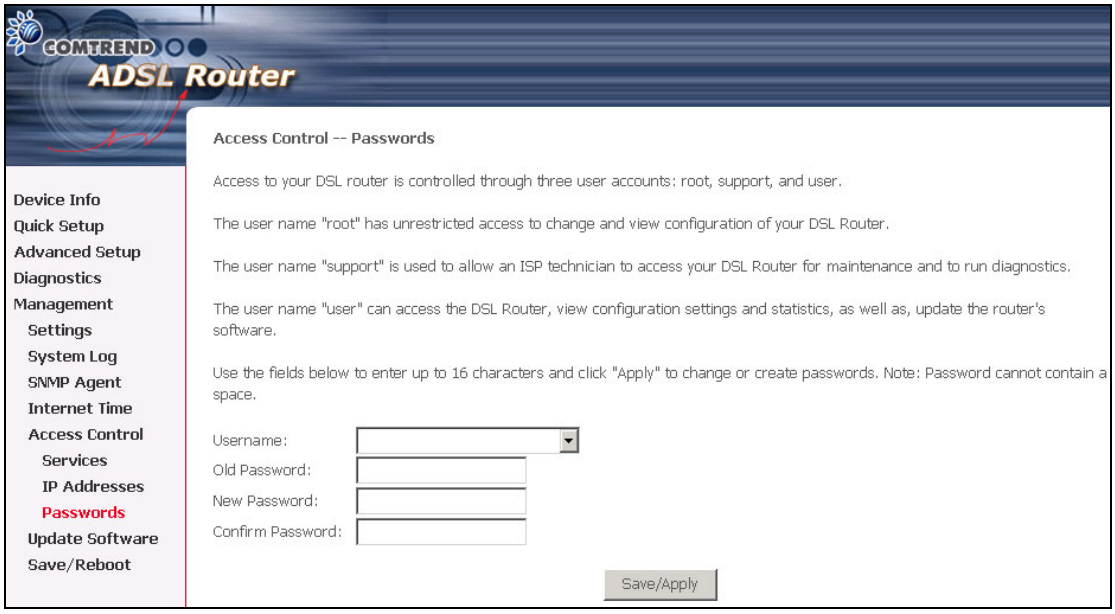
Enter the IP address and click **Apply** to allow the PC with this IP address to manage the router.

9.5.3 Passwords

The Passwords option configures the access passwords for the router. Access to your DSL router is controlled through the following user accounts:

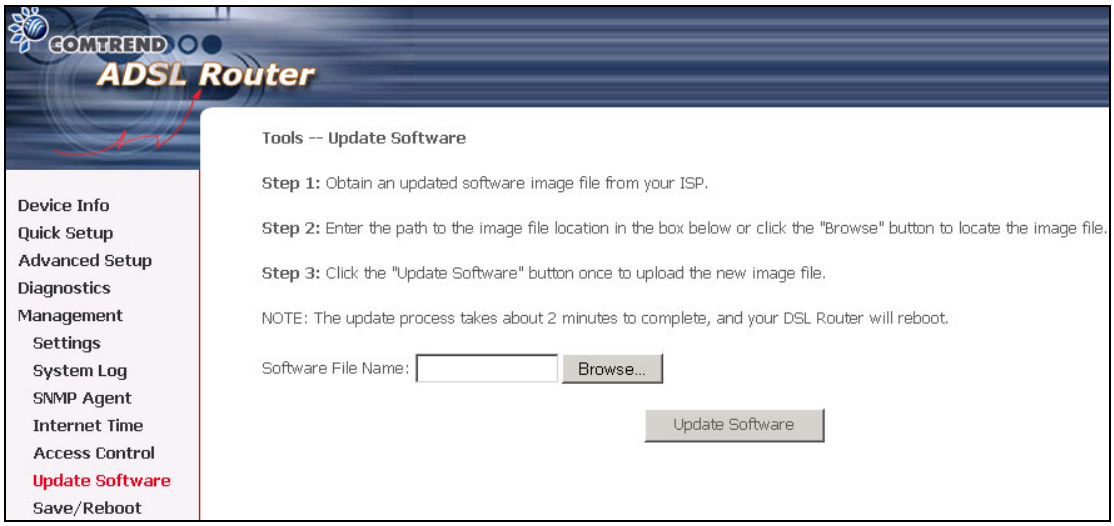
- **root** has unrestricted access to change and view the configuration
- **support** is used for remote maintenance and diagnostics.
- **user** has limited access to device information, statistics and software updates.

Use the fields below to enter up to 16 characters and click **Save/Apply** to change or create passwords.



9.6 Update software

The Update Software screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.



Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE:	The update process takes about 2 minutes to complete since the router must reboot.

9.7 Save and Reboot

The Save/Reboot options saving the configurations and reboot the router. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Appendix A: Firewall

Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3.
When a Routing interface is created "Enable Firewall" must be checked.
Navigate to Advanced Setup -> Firewall -> IP Filtering, web page.

Outgoing IP Filtering: Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP.

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.
Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.
Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Examples:

1.
Filter Name	: Out_Filter1
Protocol	: TCP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Dest. Address	: Null
Dest. Sub. Mask	: Null
Dest. Port	: Null

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2. Filter Name : Out_Filter2
   Protocol : UDP
   Source Address : 192.168.1.45
   Source Subnet Mask : 255.255.255.0
   Source Port : 5060:6060
   Dest. Address : 172.16.13.4
   Dest. Sub. Mask : 255.255.255.0
   Dest. Port : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub.Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070

Incoming IP Filtering:
Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IPtraffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.
Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular
"Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

Examples:

1. Filter Name : In_Filter1
   Protocol : TCP
   Source Address : 210.168.219.45
   Source Subnet Mask : 255.255.0.0
   Source Port : 80
   Dest. Address : Null
   Dest. Sub. Mask : Null
   Dest. Port : Null

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface

mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2. Filter Name : In_Filter2
   Protocol : UDP
   Source Address : 210.168.219.45
   Source Subnet Mask : 255.255.0.0
   Source Port : 5060:6060
   Dest. Address : 192.168.1.45
   Dest. Sub. Mask : 255.255.255.0
   Dest. Port : 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub.Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:
These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Firewall -> MAC Filtering web page.

Global Policy:
When set to Forwarded the default filter behavior is to
Forward all MAC layer frames except those explicitly stated in the rules.
Setting it to Blocked changes the default filter behavior to Drop all
MAC layer frames except those explicitly stated in the rules.

To setup a rule:

Protocol Type: Can be either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI or IGMP.

Destination MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Source MAC Address: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

Frame Direction:
LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.
WAN => LAN --> All Frames coming from WAN destined to LAN.
LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

Example 1:
Global Policy: Forwarded
Protocol Type: PPPoE
Dest. MAC Addr: 00:12:34:56:78
Source MAC Addr: Null
Frame Direction: LAN => WAN
WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78 irrespective of its Source MAC Addr. on the br_0_34 WAN interface. All other frames on this interface are forwarded.

Example 2:
Global Policy: Blocked
Protocol Type: PPPoE
Dest. MAC Addr: 00:12:34:56:78:90
Source MAC Addr: 00:34:12:78:90:56
Frame Direction: WAN => LAN
WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Appendix B: Pin Assignments

Line Port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix C: Specifications

Rear Panel

RJ-11 X1 for ADSL, RJ-45 X 4 for LAN, Power Button X 1, Reset Button X 1

ADSL

ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2

G.992.5 (ADSL2+)	Downstream : 24 Mbps	Upstream : 1.3 Mbps
G.992.3 (ADSL2)	Downstream : 12 Mbps	Upstream : 1.3 Mbps
G.DMT	Downstream : 8 Mbps	Upstream : 832 Kbps

Ethernet

Standard	IEEE 802.3, IEEE 802.3u
10/100 BaseT	Auto-sense
MDI/MDX support	Yes

ATM Attributes

RFC 2364 (PPPoA);RFC 2684 (RFC 1483)
Bridge/Route;RFC 2516 (PPPoE); RFC 1577 (IPoA)

Support PVCs	8
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1/4.0
OAM F4/F5	Yes

Management

SNMP, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP, TFTP or FTP server.

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
VLAN support	Yes
Spanning Tree Algorithm	Yes
IGMP Proxy	Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DHCP Client/Server, DNS Proxy, ARP

Security Functions

Authentication protocols: PAP, CHAP
TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet Filtering, Access Control

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc.

Power Supply

External power adapter 110 Vac or 220 Vac

Environment Condition

Operating temperature 0 ~ 50 degrees Celsius
Relative humidity 5 ~ 90% (non-condensing)

Dimensions

140 mm (W) x 40 mm (H) x 133 mm (D)

NOTE: Specifications are subject to change without notice